VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

Diplomová práce

2012 Bc. Radim Vašíček

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Rozhodnutelné podtřídy formulí predikátového počtu 1. řádu

Decidable Subclasses of Formulae of the 1st-order Predicate Calculus

2012 Bc. Radim Vašíček

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Radim Vašíček**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Rozhodnutelné podtřídy formulí predikátového počtu 1. řádu
Decidable Subclasses of Formulae of the 1st-order Predicate Calculus

Zásady pro vypracování:

Cílem práce je vypracovat studii o rozhodnutelných podtřídách formulí predikátové logiky 1. řádu.

1. Student prostuduje literaturu dle pokynů vedoucího práce o problému (částečné) rozhodnutelnosti či nerozhodnutelnosti logické pravdivosti formulí predikátové logiky 1. řádu.
2. Na základě získaných poznatků vypracuje přehlednou studii, která bude pro každou rozhodnutelnou podtřídu obsahovat jasné zdůvodnění, proč je rozhodnutelná.
3. Student vypracuje příklady, kdy důkazový postup nerozhodne formuli, která nesplňuje omezení dané podtřídy.
4. Výsledky budou zpracovány ve formě webové prezentace tak, aby byly použitelné pro výuku v kursu Vybrané partie z matematické logiky.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. RNDr. Marie Duží, CSc.**

Datum zadání: 18.11.2011

Datum odevzdání: 04.05.2012

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky * OSTRAVA *

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

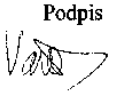
Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 3. 5. 2012

Radim Vašíček

Podpis



Poděkování

Na tomto místě bych rád poděkoval vedoucí své diplomové práce paní Doc. RNDr. Marii Duží, CSc, za odbornou pomoc, konzultaci a cenné rady, které pro mne byly velkým přínosem při vytváření této práce.

Abstrakt

Pro predikátovou logiku prvního řádu existují úplné a samozřejmě bezesporné důkazové kalkuly. Dle věty o úplnosti Kurta Gödela lze vyvinout kalkul (např. Hilbertův), ve kterém je každá logicky pravdivá formule dokazatelná a navíc (dle silnější verze věty o úplnosti), pokud daná formule logicky vyplývá ze zvolených axiomů, pak je z nich dokazatelná. Avšak neexistují kalkuly, ve kterých by bylo možno rozhodnout, zda je daná formule logicky pravdivá či zda je důsledkem zvolených axiomů, což je jedním z důsledků první Gödelovy věty o neúplnosti. Proto říkáme ve zkratce, že predikátová logika 1. řádu není rozhodnutelná. Nicméně existuje celá řada podtříd formulí predikátového počtu prvního řádu, které mají tuto žádoucí vlastnost, jsou rozhodnutelné. Cílem této diplomové práce je vypracovat přehlednou studii o těchto podtřídách formulí predikátové logiky 1. řádu a následně tyto výsledky zpracovat do podoby webové stránky tak, aby bylo možné výsledky využít pro výuku předmětu vybrané partie z matematické logiky. Navíc lze pak tyto výsledky uplatnit v teorii a praxi automatizovaného dokazování teorémů.

Klíčová slova

Predikátová logika prvního řádu, bezespornost, úplnost, rozhodnutelnost, rozhodnutelné podtřídy, entscheidungsproblem

Abstract

Complete and, of course, indisputable proof calculi exist for the first-order predicate logic. By Kurt Gödel's completeness theorem, a calculus (such as the Hilbert Calculus) with the following property can be developed: Each logical true formula is provable and (by the stronger version of the completeness theorem) if a given formula logically follows from given axioms, then it is provable from these axioms. There are not, however, any calculi where it would be possible to decide whether or not a given formula is logically true or whether it is the consequence of a given set of axioms. This is one of the implications of Gödelov's first incompleteness theorem. Therefore, we say in short that the first-order predicate logic is undecidable. There are however a large number of predicate calculus formulae subclasses that have the desirable property of being decidable. The goal of this diploma thesis has been to compile a synoptic study of such first-order predicate logic formulae subclasses and put it into the form of a webpage so that the results are accessible for teaching the subjects of select parts of mathematical logic. These results can also find further application in the theory and practice of automated proving of theorems.

Keywords

First-order predicate logic, consistency, completeness, decidability, decidable subclasses, entscheidungsproblem

Seznam použitých symbolů a zkratek

PL1	predikátová logika prvního řádu
PL2	predikátová logika druhého řádu
DUF	množina všech dobře utvořených formulí
SAT	problém splnitelnosti logických formulí (satisfiability problem - SAT)
Fin-Sat	problém konečné splnitelnosti logických formulí
Thm(T)	theorems of T - teorie sentencí struktury T
Th(N)	teorie modelu N
DNF	disjunktivní normální tvar
CNF	konjunktivní normální tvar

Obsah

1 Úvod

Cílem této diplomové práce je zmapování problematiky logické pravdivosti formulí v predikátové logice prvního řádu a vypracování přehledné studie o rozhodnutelných podtřídách formulí PL1. Obecně je známo, že predikátová logika prvního řádu je nerozhodnutelná. Nicméně existují tzv. fragmenty (třídy) predikátové logiky prvního řádu, ve kterých je problém logické pravdivosti formulí rozhodnutelný.

1.1 Původní problém

Původní *klasický rozhodovací problém* je možné formulovat několika ekvivalentními způsoby.

- *Problém splnitelnosti* (nebo *problém konzistentnosti*) v logice prvního řádu: pro danou formuli (množinu formulí) prvního řádu rozhodneme, zda je konzistentní.

- *Problém platnosti* u logiky prvního řádu: u dané formule prvního řádu rozhodneme, zda je logicky platná.

- *Problém dokazatelnosti* u řádného a kompletního dokazovacího systému pro logiku prvního řádu: u dané formule prvního řádu rozhodneme, zda je v systému dokazatelná.

Vzpomeňme si, že nějaká formule je *splnitelná* (neboli *konzistentní*), pokud má model. Je *validní* (nebo taky *logicky pravdivá*), pokud zůstává platnou ve všech modelech, ve kterých je definovaná. Nějaký důkazový systém je *přesvědčivý (angl. „sound“),* pokud každá dokazatelná formule je platná; je *úplný,* pokud každá logicky platná formule je dokazatelná.

Byl to právě Hilbert, kdo zaměřil pozornost matematiků na klasický rozhodovací problém a udělal z něj centrální problém matematické logiky. Nazýval jej *„das Entscheidungsproblem“*, což doslovně znamená „rozhodovací problém“. Na začátku tohoto století vyvíjel formalistický program pro základy matematiky a zajímal se tudíž o axiomatizaci rozdílných odvětví matematiky finitní metodou, tj. na základě konečného počtu schémat axiomů prvního řádu. V principu taková axiomatizace redukuje důkaz matematického tvrzení na vykonání mechanické derivace ve fixovaném formálním logickém systému; viz níže. Očividně je *Entscheidungsproblem* velmi důležitý v tomto kontextu:

> *...otázka konzistence se prezentuje jako problém čisté predikátové logiky...Takováto otázka...spadá pod „Entscheidungsproblem“. [22, strana 8]*

Hilbert a Ackermann formulovali přesvědčivý formální důkazový systém pro logiku prvního řádu a odhadli, že tento systém je úplný, což dokázal Gödel ve své diplomové práci 1930. Silná Gödelova věta o úplnosti pak říká, že každá sentence, která je pravdivá ve všech modelech axiómů, je z těchto axiómů dokazatelná. Důkaz se nachází ve standardních učebnicích, jako např. [24, 25, 26, 27, 28]. Pro naše potřeby nenesou detaily formálního systému žádný význam. Budeme jednoduše

předpokládat, že některé přesvědčivé a kompletní formální důkazové systémy byly pro logiku prvního řádu opraveny. Všimněte si, že existuje mechanická procedura, která derivuje všechny validní formule prvního řádu v nějakém pořadí.

Abychom si vysvětlili, jak se důkaz matematického tvrzení redukuje na matematickou derivaci, předpokládejte, že *T* je konečně axiomatizovatelná matematická teorie. Bez ztráty obecnosti nemají axiomy žádné volné individuální proměnné (tzn., jde o sentence). Vskutku, pokud má nějaký axiom volné individuální proměnné, nahraďte jej jeho universálním uzávěrem (closure). Nechť α je konjunkcí axiomů, β další sentencí prvního řádu (matematické tvrzení v terminologii Hilberta) a nechť γ je implikací $\alpha \supset \beta$. Potom β je větou z *T* tehdy a právě tehdy, pokud je γ validní, a pouze tehdy, pokud je γ dokazatelná ve fixovaném formálním důkazovém systému. Matematická otázka, zda je β větou z *T,* je tak redukována na logickou otázku: zda je γ dokazatelná z množiny daných axiómů. Tato otázka se dále redukuje na otázku, zda dříve zmíněná mechanická procedura derivuje formuli γ.

Mnoho důležitých matematických problémů se tímto způsobem redukuje na logiku. Přidejme další příklad.

Příklad. Redukce Riemannovy hypotézy na problém platnosti pro nějakou sentenci γ prvního řádu. Vzpomeňte si, že Diophantova rovnice, je rovnice $P(x_1, \ldots, x_k) = 0$, kde P je polynom s celočíselnými koeficienty a rozsahem proměnných x_i přes celá čísla. V [23] autoři ukazují Diophantovu rovnici *E,* která je řešitelná tehdy a právě tehdy, pokud Riemannova hypotéza selže. Dostačuje nalézt konečně axiomatizovatelnou teorii T a sentenci β takovou, že β je dokazatelná v *T* tehdy a jen tehdy, pokud je *E* řešitelné. Požadované γ je potom implikací $\alpha \supset \beta$, kde α je konjunkcí (universálně uzavřených) axiomů z *T*.

Připomeňme, že standardní (přirozená) aritmetika *A* je teorie nad množinou přirozených čísel se zvláštními znaky pro číslo 0, funkci následníka, sčítání, násobení a relaci uspořádání $\leq$.. Aritmetika *A* obsahuje všechny formule pravdivé ve standardním modelu. Nechť *L* je jazyk prvního řádu. Robinsonova aritmetika *Q* je finitní axiomatická teorie v *L*, pro kterou platí, že existenční *L*-sentence φ je dokazatelná v *Q* tehdy a jen tehdy, pokud platí v *A*. (Podobná teorie se nazývá *N* v[28]). Zvolme *T* tak, aby bylo totožné s *Q*. Pak je dostačující zkonstruovat existenční *L*-sentenci β takovým způsobem, že *E* je řešitelné tehdy a jen tehdy, pokud β nepřestává platit v *A*.

Fakticky je možné vyjádřit libovolnou Diophantovskou rovnici *D* nějakou existenční formulí β_D. Jelikož je disjunkce existenčních sentencí ekvivalentní existenční sentenci, je dostačující zkontrolovat, že nějaká existenční *L*-sentence může vyjádřit danou rovnici $P(x_1, \ldots, x_k) = 0$ společně s atomickou mezí $x_i \geq 0$ nebo $x_i \leq 0$, pro každou proměnnou x_i. Toto je ovšem zřejmé.

Např. rovnice $x^3 - y^5 + 1 = 0$ s mezemi $x \leq 0$, $y \leq 0$ je ekvivalentní nějaké rovnici $(-x)^3 - (-y)^5 + 1 = 0$ s mezemi $x \geq 0$, $y \geq 0$, což je ekvivalentní rovnici $y^5 + 1 = x^3$ s mezemi $x \geq 0$, $y \geq 0$, což je očividně vyjádřitelné nějakou existenční *L*-sentencí.

Hilber a Ackermann nazývají klasický rozhodovací problém hlavním problémem matematické logiky:

> *Entscheidungsproblem bude vyřešen, až budeme znát proceduru, která umožňuje rozhodnout u jakéhokoliv daného logického výrazu v konečném počtu operací jeho platnost či splnitelnost. (...) Entscheidungsproblem je třeba považovat za hlavní problém matematické logiky.*

Hilbert a Ackermann nebyli sami ve svém docenění důležitosti klasického rozhodovacího problému. Jejich postoj byl sdílen dalšími předními logiky jejich doby. Bernays a Schöfinkel napsali:

> *Centrálním problémem matematické logiky, který se rovněž úzce vztahuje k otázkám axiomatiky, je Entscheidungsproblem.* [29].

Herbrandova studie začíná takto:

> *Mohli bychom zvážit fundamentální problém matematiky. Problém A: Jaká je nezbytná a dostačující podmínka pro pravdivost nějaké věty v dané teorii, která má pouze konečný počet hypotéz?*

Studie končí:

> *Řešením tohoto problému by se získala v matematice obecná metoda a řešení by umožnilo matematické logice hrát vůči klasické matematice stejnou roli, jakou hraje vůči běžné geometrii geometrie analytická.*

V [46], Herbrand dodává:

> *V jistém smyslu je [klasický rozhodovací problém - BGG] nejobecnějším problémem matematiky.*

Ramsey napsal, že se jeho studie

> *zabývala speciálním případem jednoho z nejvýznamnějších problémů matematické logiky, a sice problémem nalezení regulární procedury pro určení pravdy či nepravdivosti kterékoliv dané logické formule. [30, str. 264]*

Kořeny klasického rozhodovacího problému je možné dohledat i v nedávné minulosti.

Filozofové se zajímali o obecnou metodu na řešení problémů. Středověký myslitel Raimundus Lullus takovou metodu nazýval *ars magna*. Leibniz byl první, kdo si uvědomil, že obsáhlý a přesný symbolický jazyk (*characteristica universalis*), je nutným předpokladem jakékoliv obecné metody na řešení problémů. Přemýšlel o diferenciálním a integrálním počtu (*calculus ratiocinator*) jako nástroji k mechanickému řešení otázek formulovaných v univerzálním jazyku. Univerzální symbolický jazyk omezený na matematiku musel počkat až do roku 1879, kdy Frege publikoval [31]; tento jazyk umožnil Russelovi a Whiteheadovi virtuálně zakotvit celé těleso - tehdy známé matematiky - do formálního rámce. Leibniz rozlišoval mezi dvěma verzemi *ars magna*. První verze, *ars inveniendi*, která nachází všechna pravdivá vědecká tvrzení. Druhá, *ars iudicandi*, nám umožňuje rozhodnout, zdali je nějaké vědecké tvrzení pravdivé či nikoliv.

V rámci logiky prvního řádu, jistá *ars inveniendi* existuje: kolekce logicky pravdivých formulí prvního řádu je rekurzivně vyčíslitelná, a tudíž existuje algoritmus, který vrátí všechny logicky pravdivé formule. Na klasický rozhodovací problém lze nahlížet jako na problém *ars iudicandi* v prvořádovém rámci. Lze jej zaostřit na otázku s odpovědí ano či ne: Existuje algoritmus, který rozhodne o logické pravdivosti jakékoliv dané formule predikátové logiky prvního řádu? Někteří logici byli skeptičtí, že takový algoritmus bude kdy nalezen. Nebylo nicméně jasné, zda bylo možné skepticismus ospravedlnit matematickou větou. John von Neumann napsal:

> *Zdá se tak, že neexistuje způsob, jak nalézt obecné kritérium pro rozhodnutí, zdali je či není dobře utvořená formule dokazatelná. (Nemůžeme ovšem v tuto chvíli toto předvést. A skutečně — nemáme představu o tvaru takového důkazu o nerozhodnutelnosti). (. . .) Tato nerozhodnutelnost je pro současnou matematickou praxi dokonce oním* ***conditio sine qua non****, jelikož svým způsobem používá heuristické metody, aby dávala smysl. Ve chvíli, kdyby přestala existovat nerozhodnutelnost, by přestala existovat i matematika, jak ji známe dnes; byla by nahrazena zcela mechanickým předpisem, pomocí kterého by kdokoli rozhodl o rozhodnutelnosti či nerozhodnutelnosti jakékoli dané sentence.*
>
> *Tudíž musíme zaujmout tento postoj; je obecně nerozhodnutelné, zda je dobře utvořená formule dokazatelná či nikoli. Jediné, co můžeme udělat je, (. . .) sestavit libovolný počet dokazatelných formulí. Tímto způsobem můžeme mnoho dobře utvořených formulí považovat za dokazatelné. Ale tímto způsobem dobře utvořenou formuli nikdy úspěšně nestanovíme jako nedokazatelnou.*

Gaelovy věty o neúplnosti byly v logice a matematice převratem a zásadně změnily tvář moderní matematiky. Je možné použít nějakou podobnou metodu k dokázání neexistence rozhodovacího algoritmu u klasického rozhodovacího problému? V apendixu spisu jménem „Fundamentální problém matematické logiky“ napsal Herbrand:

> *Všimněte si nakonec, že ačkoliv se v současnosti nezdá pravděpodobné, že problém rozhodnutelnosti je možné vyřešit, ještě nebylo dokázáno, že je to nemožné*.

Herbrand, Gödel a Kleene vyvinuli velmi obecnou představu rekurzivních funkcí [27]. V roce 1936 představil Church velmi smělou tezi: každá vyčíslitelná funkce z přirozených čísel na přirozená čísla je rekurzivní ve smyslu Herbrand-Gödel-Kleenova. Ukázal, že žádná rekurzivní funkce nemůže rozhodnout logickou pravdivost sentencí prvního řádu a došel k závěru, že neexistuje žádný rozhodovací algoritmus pro klasický rozhodovací problém.

Nezávisle představil Alan Turing výpočetní zařízení, která se dnes nazývají Turingovy stroje. Představil podobnou tezi: funkce z řetězců na řetězce je vyčíslitelná tehdy a právě tehdy, pokud je vyčíslitelná nějakým Turingovým strojem. Ukázal, že žádný Turingův stroj nedokáže rozhodnout logickou pravdivost sentencí prvního řádu a došel k závěru, že neexistuje obecný rozhodovací algoritmus pro klasický rozhodovací problém. Brzy byla dokázána ekvivalence Churchovy a Turingovy teze. Church-Turingova teze byla z velké části přijata a předpokládalo se tudíž, že ano/ne verze klasického rozhodovacího problému byla vyřešena Churchem a Turingem negativně.

1.2 Transformace klasického rozhodovacího problému

Už před příchodem Churchových a Turingových tezí měla oblast klasického rozhodovacího problému bohatou a plodnou historii. Četné fragmenty logiky prvního řádu byly prokázány rozhodnutelnými pro logickou pravdivost a četné fragmenty byly ukázány stejně složitými jako celý problém. Co znamená, že je fragment F pro (logickou) platnost stejně složitý jako celý problém? Znamená to, že existuje algoritmus A, který transformuje libovolnou formuli φ do formule v F takovým způsobem, že $A(\varphi)$ je logicky pravdivá tehdy a právě tehdy, když je logicky pravdivá φ. Takový fragment se nazývá *redukční třída* pro (logickou) platnost. Ve skutečnosti bylo obvyklejší hovořit o splnitelnosti a konečné splnitelnosti, čili splnitelnosti v nějaké konečné struktuře. Redukční třídy pro splnitelnost (respektive konečnou splnitelnost) jsou definovány podobně.[1]

Abychom ilustrovali problémy tohoto oboru, citujme některé rané výsledky ohledně fragmentů čisté predikátové logiky prvního řádu (logika prvního řádu bez funkčních symbolů a rovnosti). Připomeňme, že *prenexní* formule je, stručně řečeno, formule se všemi kvantifikátory vlevo, na začátku formule. Nahlížejme na řetězec v čtyř-písmenné abecedě $\{\forall, \exists, \forall^*, \exists^*\}$, jako na regulární výraz, který vyjadřuje kolekci řetězců v dvoupísmenové abecedě $\{\forall, \exists\}$. Např. $\forall^3\exists^*$ značí kolekci řetězců ve formě $\forall\forall\forall\exists^j$, kde j je libovolné přirozené číslo, a $\exists^*\forall^2\exists^*$ značí kolekci řetězců ve formě $\exists^i\forall\forall\exists^j$, kde i a j jsou libovolná přirozená čísla.

V roce 1915, Löwenheim zveřejnil rozhodovací proceduru pro splnitelnost predikátových formulí s pouze unárními predikáty. Dokázal rovněž, že formule s binárními predikáty tvoří redukční třídu pro splnitelnost. V roce 1931 se Herbrand zaostřil na poslední výsledek a ukázal tak, že pouze tři binární predikáty jsou dostačující. V roce 1936 nakonec Kalmár ukázal, že jeden binární predikát je dostačující.

V roce 1920 ukázal Skolem, že sentence $\forall^*\exists^*$ tvoří redukční třídu pro splnitelnost. V roce 1928 Bernays a Schönfinkel představili rozhodovací proceduru pro splnitelnost $\exists^*\forall^*$ sentencí. V roce 1928 Ackermann představil rozhodovací proceduru pro splnitelnost $\exists^*\forall\exists^*$ sentencí. Gödel, Kalmár a Schütte nezávisle na sobě v letech 1932, 1933 a 1934 (v tomto pořadí) objevili rozhodovací procedury pro splnitelnost čistých $\exists^*\forall^2\exists^*$ sentencí. V dalším spise Gödel dokázal, že každá

[1] Budu-li v dalším textu hovořit o platnosti formulí, myslím tím logickou pravdivost formule případně pravdivost v určitém zamýšleném modelu.

splnitelná $\exists^*\forall^2\exists^*$sentence má konečný model a že sentence $\forall^3\exists^*$ tvoří redukční třídu pro splnitelnost. (Viz [39] ohledně populárně naučného úvodu do klasického rozhodovacího problému.)

Reakce logiků na objevy Churche a Turinga byla, že klasický rozhodovací problém je širší než jeho ano/ne verze. Zde je jedna z prvních reakcí:

> *Takové redukce [odkaz na redukce navržené Skolemem v citovaném spisu — BGG] budou, doufejme, užitečné pro systematický výzkum formulí prvního řádu, např. pokud si někdo přeje přijít na kompletní obraz, kde třídy takových formulí opravdu dokážou vyřešit Entscheidungsproblem. Tak, jak je známo, A. Church dokázal, že obecné řešení tohoto problému není možné.*

Logikové postupně začali přemýšlet o klasickém rozhodovacím problému jako o problému klasifikačním.

- Které fragmenty jsou rozhodnutelné, co se týče splnitelnosti, a které jsou nerozhodnutelné?
- Které fragmenty jsou splnitelné, co se týče konečné splnitelnosti, a které jsou nerozhodnutelné?
- Které fragmenty mají vlastnost konečného modelu a které obsahují axiomy nekonečna (čili jsou splnitelnými formulemi bez konečných modelů)?

Dlouhou dobu zůstával klasický rozhodovací problém centrálním problémem matematické logiky. S vývojem teorie výpočtové složitosti byl problém určen blíže. Pokud je fragment logiky prvního řádu rozhodnutelný, co se týče splnitelnosti, pak opravdu existuje absolutně mechanická procedura, čili nějaký algoritmus, který dokáže rozhodnout o splnitelnosti či nesplnitelnosti kterékoliv dané sentence. Ale jaká je výpočtové složitost takového algoritmu? Podobně; pokud je nějaký fragment rozhodnutelný pro konečnou splnitelnost, jaká je výpočtové složitost určení konečné splnitelnosti?

Samozřejmě, neomezený problém klasifikovatelnosti je beznadějný. Existuje zde prostě příliš mnoho fragmentů. Některé nemají žádný význam pro nikoho. Některé zahrnují konkrétní odvětví matematiky. Zvažte např. problém splnitelnosti u sentencí $\alpha \wedge \beta$, kde α je (univerzální uzavření) konjunkce axiomů teorie okruhů a β je libovolná formule teorie polí. Tento problém právem patří do teorie pole spíše než do logiky.

Nakonec začal pojem klasický rozhodovací problém znamenat omezení klasifikačního problému popsaného výše na tradiční fragmenty. Je nutno připustit, že tento popis není přesný, ale poskytuje dostatečné vedení, které budeme následovat. Lze argumentovat, že problém úplnosti ve skutečnosti nepatří do tradičního rozhodovacího problému. Toto je také pravda, ale není možné ignorovat otázku úplnosti v této době, a to konkrétně kvůli relevanci procedur logického rozhodování vůči metodám dokazování vět a ověřování modelů. Pokusíme se popsat známé výsledky o úplnosti.

Jak jsem zmínil výše, po dlouhou dobu zůstával klasický rozhodovací problém centrálním problémem matematické logiky. Literatura na toto téma je rozsáhlá a obsahuje značné množství zají-

mavých materiálů. Klasický rozhodovací problém sloužil jako laboratoř logických metod a zvláště pak metod redukčních. Klasifikační výsledky byly použity nejen v logice ale také v teoretické informatice. Konkrétně byly použity jako průvodce studia zákonů jedniček a nul pro fragmenty logiky druhého řádu. Klasické techniky inspirovaly některé důkazy zákonů jedniček a nul a některé z klasických technik byly dále rozšířeny.

Existuje množství knih věnujících se problému klasické rozhodnutelnosti. V padesátých letech dvacátého století podal Ackermann rozsáhlé zpracování do té doby známých řešitelných případů [18], Surányi podal alternativní rozsáhlé zpracování do té doby známých tříd redukce. Kniha [41] od autorů Drebena a Goldfarba ilustruje potenciál tzv. Herbrandovy techniky expanze ve stanovení řešitelnosti. Doplňující kniha [42] od Lewise pokrývá mnoho výsledků redukce na klasických částech čisté predikátové logiky. Dohromady tyto dvě knihy podávají systematické zpracování problémů rozhodnutelnosti pro predikátovou logiku bez funkcí nebo rovnosti.

Nicméně mnoho z tohoto bohatství se nikdy v knižní formě neobjevilo. Navíc v této době je již práce na problémech klasické rozhodnutelnosti z většiny hotova (některé problémy samozřejmě přesto stále zůstávají otevřené) a většina hlavních klasifikací přesto nikdy nebyla uvedena v knižní podobě.

1.3 Co je obsahem této diplomové práce?

Největší pozornost věnuji nejtradičnějším částem predikátové logiky prvního řádu, a to konkrétně souborům prenexních formulí daných omezeními kvantifikátorového prefixu „a / nebo“ slovní zásoby. (Připomeňme, že existuje jednoduchý algoritmus převodu libovolné formule prvního řádu na ekvivalentní formuli v prenexní formě.)

Řetězce ve dvouznakové abecedě $\{\forall,\exists\}$ budeme nazývat *prefixy*. *Prefixová množina* bude množina všech prefixů. *Posloupnost arity* je funkce p z množiny přirozených čísel do množiny nezáporných celých čísel rozšířených o první nekonečný ordinál ω.

Definice (Třídy prefixové slovní zásoby). Pro libovolnou prefixovou množinu Π a libovolné posloupnosti arity p, f $[\Pi, p, f]$ (resp. $[\Pi, p, f]_{=}$) je soubor všech prenexních formulí φ logiky prvního řádu bez rovnosti (resp. s rovností) takový, že:

- prefix formule φ náleží do množiny Π,
- počet n-árních predikátových symbolů formule φ je $\leq p(n)$ a
- počet n-árních funkčních symbolů formule φ je $\leq f(n)$.
- formule φ nemá žádné nulární predikátové symboly (0 - konstanta nula) s výjimkou logických konstant *pravda* a *nepravda*, žádné nulární funkční symboly a žádné volné proměnné.

Vysvětleme si poslední podmínku. Budeme hovořit o logice bez rovnosti, avšak to samé lze aplikovat také na logiku s rovností. Je jednoduché zpozorovat, že se stav (rozhodnutelný nebo ne-

rozhodnutelný) problému (konečné) splnitelnosti pro třídy prefixové slovní zásoby nezmění, pokud povolíme nulární predikátové symboly. Zvažme nyní roli nulárních predikátových symbolů neboli samostatných konstant. Nechť C = [*Π, p, f*] a nechť C′ je taková verze C, kde je dovoleno použít řekněme 7 samostatných konstant. Je jednoduché zpozorovat, že stav problému (konečné) splnitelnosti pro C′ je shodný se stavem problému (konečné) splnitelnosti pro [*Π′, p, f*], kde $\Pi' = \{\exists^7\pi : \pi \in \Pi\}$. Místo o samostatných konstantách můžeme hovořit o volných samostatných proměnných. Povolení samostatných konstant či volných samostatných proměnných nám tak stejně více tříd rovněž nepřidá. Výše uvedená definice tříd prefixového slovníku se zdá být příliš obecná.

Řekneme, že prefixová množina je *uzavřená,* pokud obsahuje všechny (i nesousední) subřetězce svých prefixů. Zřejmě můžeme svou pozornost zaměřit na uzavřené prefixové množiny. Dále řekneme, že prefixová množina *Π* je *standardní,* pokud se buďto jedná o množinu všech prefixů nebo může být zadána řetězcem *w* čtyř-písmenné abecedy {∀, ∃, ∀*, ∃*}. V prvním případě množiny Π je třeba zdůraznit slovo *všech*. Tedy, každá standardní prefixová množina má stručný zápis. Dále můžeme bez újmy na obecnosti požadovat, aby *w* bylo *redukované* v následujícím smyslu: ∀* nemůže mít za „souseda“ ∀ a stejně tak ∃* nemůže mít za „souseda“ ∃. Například řetězec ∀*∀∃∃* se zredukuje na řetězec ∀*∃*; tyto dva řetězce očividně definují stejnou prefixovou množinu.

Nazývejme posloupnost arity *p standardní*, pokud splňuje následující vztah: $p(n) = \omega$, a to kdykoliv, kdy je součet $p(n) + p(n + 1) + \ldots$ nekonečný. Každé standardní notaci lze přiřadit její stručný zápis. Standardní posloupnost arity, která přiřazuje ω libovolnému *n*, bude označena jako *all*. Jakákoliv jiná standardní posloupnost *p* končí řadou nul, $0 = p(m) = p(m+1) = \ldots$..a bude určena posloupností $(p(1), p(2), \ldots, p(m-1))$. V případě $m = 1$ z důvodu čitelnosti raději označíme *p* nulou (0) než prázdnou závorkou (). Stejný zápis může být použit pro nestandardní posloupnosti končící řadou nul. Povšimněme si, že každou posloupnost arity lze zredukovat na standardní posloupnost arity. Například, [*all*, (0, ω), (0)] ⊆ [*all*, (ω, ω), (0)] a každá sentence φ∈ [*all*, (ω, ω), (0)] může být jednoduše přepsána jako ekvivalentní sentence v [*all*, (0, ω), (0)]: jednoduše nahraďme formule R(x), formulemi R′(x, x), kde R′ je binární predikátový symbol, který se nevyskytuje ve φ.

Definice. Řekneme, že třída prefixového slovníku [*Π, p, f*] nebo $[\Pi, p, f]_=$ je *standardní,* jestliže *Π, p* a *f* jsou standardní.

Problém klasifikace pro části prefixové slovní zásoby připouští kompletní řešení ve tvaru nějaké konečné tabulky. Speciálně, existuje pouze konečně mnoho minimálních nerozhodnutelných částí obsahujících uzavřené prefixové množiny a všechny tyto minimální části jsou standardní. Toto vyplývá z Gurevichovy věty o klasifikovatelnosti. Proto tedy budou v hlavní části diplomové práce mezi třídami prefixového slovníku, které nás budou zajímat, téměř výhradně standardní třídy.

Shrňme si tedy na závěr stručně obsah této diplomové práce: druhá kapitola je věnována obecnému výkladu predikátové logiky prvního řádu a vysvětlením dalších důležitých pojmů, které jsou v diplomové práci zmíněné. V třetí kapitole se zaměřuji na obecné vysvětlení rozhodnutelnosti a nerozhodnutelnosti formulí predikátové logiky prvního řádu a predikátové logiky obecně. Poslední

- čtvrtá kapitola – obsahuje přehled sedmi maximálním, rozhodnutelných tříd, ve kterých je problém logické pravdivosti formulí rozhodnutelný.

2 Predikátová logika prvního řádu

Při tvorbě této kapitoly jsem vycházel především z dostupných skript pro matematickou logiku a z přednášek paní Doc. RNDr. Marie Duží, CSc. Dále jsem využil knihu pana Vítězslava Švejdara: *Logika s podtitulem neúplnost, složitost a nutnost* [3]. A nakonec jsem použil materiály s názvem: *predikátová logika* [40][56], které vytvořil pan Prof. RNDr. Petr Štěpánek, DrSc. z Matematicko-fyzikální fakulty UK. Jedná se o skripta a přednášky pro předmět *výroková a predikátová logika*.

Predikátová logika 1. řádu (zkráceně také PL1), formalizuje úsudky o vlastnostech předmětů a vztazích mezi předměty pevně dané předmětné oblasti (univerza). PL1 se nezabývá formalizací úsudků, které navíc vypovídají i o vlastnostech vlastností a vztahů a o vztazích mezi vlastnostmi a vztahy. Tímto se zabývají predikátové logiky druhého a vyšších řádů. PL1 je zobecněním výrokové logiky, kterou můžeme považovat za logiku nultého řádu. Predikátová logika 1. řádu je postačující pro formalizaci mnohých matematických i jiných teorií.

2.1 Jazyk predikátové logiky

Níže si představíme obecný jazyk predikátové logiky.

I) ***Abeceda predikátové logiky*** je tvořena následujícími skupinami symbolů:

a. Logické symboly
   i. předmětové (individuové) proměnné: *x, y, z*,... (příp. s indexy)
   ii. symboly pro spojky: $\neg, \wedge, \vee, \supset, \equiv$
   iii. symboly pro kvantifikátory $\forall, \exists$
   iv. případně binární predikátový symbol = (predikátová logika s rovností)

b. Speciální symboly (určují specifiku jazyka)
   i. predikátové symboly: *P, Q, R*,... (příp. s indexy)
   ii. funkční symboly: *f, g, h*,... (příp. s indexy)
   Ke každému funkčnímu a predikátovému symbolu je přiřazeno nezáporné číslo n ($n \geq 0$), tzv. ***arita***, udávající počet individuových proměnných, které jsou argumenty funkce nebo predikátu.

c. Pomocné symboly (závorky): (,) (případně i [,],{,})

II) ***Gramatika,*** která udává, jak tvořit:

a. ***termy*:**
   i. každý symbol proměnné je term
   ii. jsou-li $t_1,\ldots,t_n$ ($n \geq 0$) termy a je-li f n-ární funkční symbol, pak výraz $f(t_1,\ldots,t_n)$ je term; pro $n = 0$ se jedná o nulární funkční symbol, neboli individuovou konstantu (značíme a, b, c, …); pro n > 0 se jedná o složený term.

iii. jen výrazy dle i. a ii. jsou termy

b. ***atomické formule***:
   i. je-li p n-ární predikátový symbol a jsou-li $t_1,\ldots,t_n$ termy, pak výraz $p(t_1,\ldots,t_n)$ je atomická formule
   ii. jsou-li t_1 a t_2 termy, pak výraz $(t_1 = t_2)$ je atomická formule

c. ***formule*:**
   i. každá atomická formule je formule
   ii. je-li výraz A formule, pak $\neg$A je formule
   iii. jsou-li výrazy A a B formule, pak výrazy (A $\vee$ B), (A $\wedge$ B), (A $\supset$ B), (A $\equiv$ B) jsou formule
   iv. je-li x proměnná a A formule, pak výrazy $\forall x$A a $\exists x$A jsou formule
   v. jen výrazy dle i. – iv. jsou formule

Následující poznámky se vztahují k výše uvedenému výkladu jazyka predikátové logiky.

Poznámky

1. Jazyk predikátové logiky - jak byl vymezen výše - je jazyk logiky 1. řádu, pro něhož je charakteristické to, že jediný přípustný typ proměnných jsou individuové proměnné. Pouze individuové proměnné lze vázat kvantifikátory. (V logice 2. řádu jsou povoleny i predikátové proměnné.).

2. Definice jazyka umožňuje formulaci speciálního jazyka (určité teorie) konkrétní volbou prvků (predikátových a funkčních konstant) dle bodu I) b. definice. Pro takový konkrétní jazyk budou platit obecné principy logické a mimo to – v závislosti na specifických vlastnostech (interpretacích) těchto prvků – i principy mimologické, které zadá tvůrce tohoto speciálního jazyka pomocí speciálních axiómů (dané teorie). Je-li arita funkčního symbolu n = 0, pak se jedná o individuovou konstantu (značíme a, b, …), která však není pravou (logickou) konstantou, neboť podléhá (jako každý funkční symbol) interpretaci.

3. Zápis formulí můžeme zjednodušit na základě následujících konvencí o vynechávání závorek:
   - Elementární formule a formuli nejvyššího řádu netřeba závorkovat (vnější závorky vynecháváme).
   - Závorky je možné vynechávat v souladu s následující prioritní stupnicí funktorů: ($\forall$, $\exists$), $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$. Každý funktor vlevo od vybraného funktoru váže silněji než vybraný funktor.
   - V případě, že o prioritě vyhodnocení nerozhodnou ani závorky ani prioritní stupnice, vyhodnocujeme formuli zleva doprava.
   - Speciálně vzhledem k asociativitě konjunkce a disjunkce, netřeba při zápisu vícečlenných konjunkcí a disjunkcí užívat žádné závorky.
   - Vedle závorek (,), lze užívat i závorky [,], {,}.

***Příklad*:** Jazyk elementární aritmetiky je případem jazyka predikátové logiky prvního řádu s rovností. Má tyto (speciální) funkční symboly:

nulární symbol: 0 (konstanta nula)

unární symbol: s (funkce následník)
binární symboly: + a × (sčítání a násobení)

Příkladem termů jsou (používáme infixní notaci pro + a ×):

0, $s(x)$, $s(s(x))$, $(x + y) \times s(s(0))$, atd.

Formulemi jsou např. výrazy:

$s(0) = (0 \times x) + s(0)$, $\exists x\,(y = x \times z)$, $\forall x\,[(x = y) \supset \exists y\,(x = s(y))]$

2.2 Definice vázané a volné proměnné, uzavřenost formule …

Výskyt proměnné x ve formuli* A *je vázaný, jestliže je součástí nějaké podformule $\forall x\mathrm{B}(x)$ nebo $\exists x\mathrm{B}(x)$ formule A.

Proměnná x je vázaná ve formuli A, má-li v A vázaný výskyt. Výskyt proměnné x ve formuli A, který není vázaný, nazýváme volný.

Proměnná x je volná ve formuli A, má-li v A volný výskyt.

Formule, v níž každá proměnná má buď všechny výskyty volné, nebo všechny výskyty vázané, se nazývá formulí s čistými proměnnými.

Formule se nazývá uzavřenou, neobsahuje-li žádnou volnou proměnnou. Formule, která obsahuje alespoň jednu volnou proměnnou, se nazývá otevřenou.

Nechť $x_1, x_2, \ldots, x_n$ jsou všechny volné proměnné formule A. Potom uzavřenou formuli

$\forall \mathrm{A} =_{\mathrm{df}} \forall x_1 \forall x_2 \ldots \forall x_n \mathrm{A}$ resp. $\exists \mathrm{A} =_{\mathrm{df}} \exists x_1\, \exists x_2 \ldots \exists x_n \mathrm{A}$,

nazýváme generálním resp. existenčním uzávěrem formule A.

Symbolem $\mathrm{A}(x/t)$ označujeme formuli, která vznikne z formule A korektní substitucí termu t za proměnnou x. Má-li být substituce korektní, musí splňovat následující dvě pravidla:

- Substituovat lze pouze za volné výskyty proměnné x ve formuli A a při substituci nahrazujeme všechny volné výskyty proměnné x ve formuli A.
- Žádná individuová proměnná vystupující v termu t se po provedení substituce x/t nesmí stát ve formuli A vázanou (v takovém případě je term t za proměnnou x ve formuli A nesubstituovatelný).

Symbolem $\mathrm{A}(x_1, x_2,\ldots,x_n / t_1, t_2,\ldots, t_n)$ označujeme formuli, která vznikne z formule A korektními substitucemi x_i/t_i pro $i = 1, 2,\ldots,n$.

Všechny formule tvaru $A(x_1, x_2,..., x_n / t_1, t_2,..., t_n)$ nazýváme instancemi formule A.

Příklad: Nechť formulí A(x) je: $P(x) \supset \forall y Q(x, y)$ a term t nechť je $f(y)$. Provedeme-li substituci A($x/f(y)$), dostaneme: $P(f(y)) \supset \forall y Q(f(y), y)$. Vidíme, že druhý (zvýrazněný) výskyt proměnné y není volný (přitom původně zde byla volná proměnná x, takže jsme změnili „smysl výrazu"). Tedy term f(y), není substituovatelný za x v dané formuli A.

2.3 Sémantika PL1 – interpretace formulí.

Sémantika - neboli význam formulí predikátové logiky 1. řádu - je dána jejich interpretací. Než tento pojem přesně definujeme, uvedeme několik neformálních motivací a vysvětlení. Položíme-li si otázku, zda daná formule PL1 je pravdivá či ne, pak taková otázka je v podstatě nesmyslná, pokud nevíme, co formule znamená, tedy jak je interpretována, neboť formule je pouze posloupnost symbolů. Tak např. formule
$\forall x P(f(x), x)$

může „říkat", že pro všechna přirozená čísla platí, že jejich druhá mocnina je větší než to číslo, nebo že pro všechny lidi platí, že jejich otec je starší než dotyčný člověk, pak je samozřejmě v takových interpretacích pravdivá. Může ale také znamenat, že pro všechna přirozená čísla platí, že jejich druhá mocnina je menší než to číslo, nebo že pro všechny lidi platí, že jejich otec je mladší než dotyčný člověk, pak je samozřejmě (v takové interpretaci) nepravdivá.

Např. formule, která je analýzou věty: „Někteří chytří lidé jsou líní", tedy:

$\exists x[\mathrm{Ch}(x) \wedge \mathrm{L}(x)]$,

může být interpretována, jako zachycující význam věty Některá lichá čísla jsou dělitelná dvěma, a pak je evidentně (v této interpretaci) nepravdivá.

V čem tedy spočívá interpretace formule? Nejprve musíme stanovit, „o čem mluvíme", tedy jaká je předmětná oblast – obor proměnnosti (individuových) proměnných, tj. zvolíme jistou neprázdnou množinu – **universum diskursu**, jejíž prvky jsou **individua**. Jelikož predikátové symboly mají vyjadřovat vztahy mezi těmito předměty, tj. prvky universa, přiřadíme každému n-árnímu **predikátovému symbolu** jistou n-ární relaci (tj. podmnožinu kartézského součinu) nad universem. Specielně, jedná-li se o unární predikátový symbol (n = 1), pak přiřadíme podmnožinu universa. Podobně **funkční symboly** budou vyjadřovat n-ární funkce nad universem. Teprve poté, co je daná formule interpretována, můžeme **vyhodnotit** její **pravdivost** či nepravdivost v **dané interpretaci**. Je zde však ještě jeden problém, a to jsou proměnné. Proměnným jazyka PL1 přiřazujeme valuací individua, tj. prvky universa. (Proměnným jazyka PL2 mohou být přiřazeny také vlastnosti či funkce).

Jak uvidíme dále z definice sémantiky kvantifikátorů, pravdivostní hodnota formule nezávisí na hodnotě vázaných proměnných (pouze volné proměnné jsou „skutečné" proměnné). Obsahuje-li však formule nějaké volné proměnné, můžeme vyhodnotit její pravdivost v dané interpretaci pouze

v **závislosti na ohodnocení** (valuaci) **volných proměnných**. Při některé valuaci může být formule v dané interpretaci pravdivá, při jiné nepravdivá. Tak např. formule

$\forall x P(\mathrm{f}(x), y)$,

může být interpretována nad množinou celých čísel tak, že symbolu p je přiřazena relace větší nebo rovno (≥), symbolu *f* funkce druhá mocnina (tedy *f* (*x*) „znamená“ x^2). Pak formule „říká”, že pro každé celé číslo *x* platí, že x^2 je větší než nebo rovno **jistému číslu *y***. Tedy pravdivost formule v této interpretaci závisí na ohodnocení (valuaci) proměnné *y*. Přiřadíme-li např. *y* číslo 5, je formule nepravdivá, přiřadíme-li třeba číslo -3 nebo 0, je formule pravdivá. Obecně bude formule pravdivá (v této interpretaci) pro každou valuaci proměnné y, která přiřadí *y* záporné číslo nebo nulu, nepravdivá pro všechny valuace, které přiřadí proměnné *y* číslo kladné.

Interpretace jazyka PL1

Interpretace jazyka predikátové logiky 1. řádu je tato trojice objektů (která je někdy nazývána interpretační struktura):

A) *Neprázdná* množina *M*, která se nazývá universum diskursu, a její prvky jsou *individua*.

B) *Interpretace funkčních symbolů* jazyka, která přiřazuje každému *n*-árnímu funkčnímu symbolu *f* určité zobrazení (*totální funkci*) f^U: $U^n \rightarrow U$.

C) *Interpretace predikátových symbolů* jazyka, která přiřazuje každému *n*-árnímu predikátovému symbolu *P* jistou *n*-ární relaci P^U nad *U*, tj. $P^U \subseteq U^n$.

Poznámky:

1. Každý *n*-ární funkční symbol je tedy interpretován jako funkce, která přiřazuje *n*-tici individuí právě jedno individuum, tj. zobrazení z $U \times ... \times U$ do *U*. Specielně:
   - je-li $n = 0$, pak se jedná o nulární funkční symbol, tedy o *individuovou konstantu*, které je interpretací přiřazen prvek universa – individuum.
   - je-li $n = 1$, pak se jedná o unární funkční symbol, kterému je přiřazena funkce o jednom argumentu (např. nad množinou čísel funkce druhá mocnina $x2$, funkce následník $x + 1$, nad množinou živých individuí funkce (biologický) otec, (biologická) matka, atd.)
   - je-li $n = 2$, pak se jedná o binární funkční symbol, kterému je přiřazena binární funkce se dvěma argumenty (např. nad množinou čísel funkce sčítání $x + y$, funkce násobení $x . y$, atd).

2. Každý *n*-ární predikátový symbol *P* je interpretován jako *n*-ární relace P_U. Tato relace P_U se nazývá *obor pravdivosti* predikátu *P*. Specielně:
   - je-li $n = 0$, pak se jedná o nulární predikátový symbol, kterému je přiřazena hodnota 1 nebo 0 (pravda, nepravda) tak, jak to již známe z výrokové logiky.

- je-li $n = 1$, pak se jedná o unární predikátový symbol, kterému je přiřazena podmnožina universa *U*. (Jak jsme již zmínili, vlastnosti v PL1 vyjadřujeme – poněkud nepřesně – jako podmnožiny universa).
- je-li $n = 2$, pak se jedná o binární predikátový symbol, kterému je přiřazena binární relace nad universem (např. relace větší, menší, mít rád, apod).

3. Výroková logika je tedy specielním (nejjednodušším) případem predikátové logiky, a to 0. řádu, ve které pracujeme pouze s nulárními predikáty a nepotřebujeme proto termy, funkční symboly, individuové proměnné ani universum diskursu (obor proměnnosti proměnných). Nulárním predikátům přiřazujeme pouze hodnoty pravda, nepravda.

Valuace jazyka PL1

Ohodnocení (neboli valuace) individuových proměnných je zobrazení e, které každé proměnné *x* přiřazuje hodnotu $e(x) \in U$ (prvek univerza).

Ohodnocení termů e^* indukované ohodnocením proměnných e je induktivně definováno takto:

$e^*(x) = e(x)$

$e^*(f(t_1, t_2,...,t_n)) = f^U (e^*(t_1), e^*(t_1),...,e^*(t_n))$,

kde f^U je funkce přiřazená v dané interpretaci funkčnímu symbolu f.

Pozn.: Hodnotou (realizací) termu t v interpretaci I je tedy vždy jistý prvek universa. Tedy funkční symboly jsou "jména funkcí – zobrazení", termy jsou "jména prvků universa", zatímco predikátové symboly jsou "jména relací" a formule jsou "jména pravdivostních hodnot".

Splnitelnost formule

- ***Formule A je splnitelná v interpretaci I***, jestliže *existuje* ohodnocení e proměnných takové, že platí $\models_I A [e]$.
- ***Formule A je pravdivá v interpretaci I***, značíme $\models_I \mathbf{A}$, jestliže pro *všechna* možná ohodnocení e individuových proměnných platí, že $\models_I A[e]$.
- ***Model formule A*** je interpretace I, ve které je A pravdivá.
- ***Formule A je splnitelná***, jestliže existuje interpretace I, ve které je splněna, tj. jestliže existuje interpretace I a valuace e takové, že $\models_I A[e]$.
- ***Formule A je tautologií*** (logicky pravdivá), značíme $\models \mathbf{A}$, jestliže je pravdivá v každé interpretaci.
- ***Formule A je kontradikcí***, jestliže nemá model, tedy neexistuje interpretace I, která by formuli A splňovala.
- ***Model množiny formulí*** $\{A_1,\ldots,A_n\}$ je taková interpretace I, ve které jsou pravdivé *všechny* formule $A_1,...,A_n$.

Důsledek.: Zjevně platí, že A je kontradikce, právě když negace *A* je tautologie, $\models \neg A$.

Formule B logicky vyplývá z formulí $\mathbf{A_1, \ldots, A_n}$, značíme $\mathbf{A_1,\ldots,A_n \models B}$, jestliže B je pravdivá v každém modelu množiny formulí $A_1,\ldots,A_n$.

Důsledek: Tedy pro každou interpretaci I, ve které jsou pravdivé formule $A_1, \ldots, A_n$ ($\models_I A_1,\ldots, \models_I A_n$) platí, že je v ní pravdivá také formule B ($\models_I B$).

2.4 Predikátová logika s rovností

Chceme-li k jazyku prvního řadu přidat predikát pro rovnost, je vhodné pro něj zavést jisté axiomy, které by zaručily, že se bude chovat tak, jak to od rovnosti intuitivně očekáváme.

Definice 2.4.1. Formální systém predikátové logiky s rovností obsahuje vše, co obsahuje formální systém predikátové logiky bez rovnosti, a navíc tyto axiomy:

- Je-li x proměnná, je následující formule axiomem identity:

$x = x$ (R1)

- Jsou-li $x_1,\ldots,x_n$ a $y_1\ldots, y_n$ proměnné a je-li f n-árni funkční symbol, potom je následující formule axiomem rovnosti pro funkce:

$x_1 = y_1 \supset x_2 = y_2 \supset \ldots \supset x_n = y_n \supset f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)$ (R2)

- Jsou-li $x_1,\ldots,x_n$ a $y_1\ldots, y_n$ proměnné a je-li p n-árni predikátový symbol, potom je následující formule axiomem rovnosti pro predikáty:

$x_1 = y_1 \supset x_2 = y_2 \supset \ldots \supset x_n = y_n \supset p(x_1,\ldots,x_n) = p(y_1,\ldots,y_n)$ (R3)

Tyto axiomy vyjadřují přirozené požadavky, které matematika klade na rovnost: aby byla reflexivní, a aby sobě rovna individua měla stejné vlastnosti vůči každému predikátu jazyka a dávala stejné výsledky při použití libovolné operace jazyka.

Protože rovnost běžně chápeme jako ekvivalenci, je přirozené po ni kromě reflexivity požadovat i další vlastnosti ekvivalence, které mezi uvedenými axiomy chybí - symetrii a tranzitivitu. Jak ale ukážu, tyto vlastnosti se ze zavedených axiomů dají odvodit. Použijeme k tomu skutečnost, že rovnost je predikát a proto může v axiomu (R3) figurovat i na místě predikátu p.

Tvrzení 2.4.2.(symetrie rovnosti). Pro libovolné proměnné x, y platí:

$\vdash x = y \supset y = x$ (SR)

Důkaz. Vyjdeme z axiomu rovnosti pro binární predikáty

$\vdash x_1 = y_1 \supset x_2 = y_2 \supset p(x_1, x_2) \supset p(y_1, y_2)$

do kterého dosadíme za x_1, y_1, x_2, y_2 po řadě x, y, x, x a za predikát p dosadíme predikát rovnosti:

$\vdash x = y \supset x = x \supset x = x \supset y = x$

Nyní použijeme větu o záměně předpokladů a první předpoklad posuneme o dvě místa doprava:

$\vdash x = x \supset x = x \supset x = y \supset y = x$

Jak je vidět, první dva předpoklady jsou axiomem identity, proto dvojím (MP) dostaneme konečně:

$\vdash x = y \supset y = x$

Tvrzení 2.4.3.(tranzitivita rovnosti). Pro libovolné proměnné *x, y, z* platí:

$\vdash x = y \supset y = z \supset x = z$ (TR)

Důkaz je podobný. Opět vyjdeme z axiomu rovnosti pro binární predikáty

$\vdash x_1 = y_1 \supset x_2 = y_2 \supset p(x_1, x_2) \supset p(y_1, y_2)$

do kterého tentokrát dosadíme za x_1, y_1, x_2, y_2 po řadě *x, x, y, z* a za predikát p opět predikát rovnosti:

$\vdash x = x \supset y = z \supset x = y \supset x = z$

Nyní opět použijeme větu o záměně předpokladů, tentokrát prohodíme druhý a třetí předpoklad:

$\vdash x = x \supset x = y \supset y = z \supset x = z$

První předpoklad je opět axiomem identity, proto pravidlem (MP) dostaneme:

$\vdash x = y \supset y = z \supset x = z$

Poznámka 2.4.4. Uvědomme si, že ačkoliv všechny tři axiomy pro rovnost i předchozí dvě tvrzení hovoří pouze o proměnných, není problém nahradit slovo „*proměnná*“ slovem „*term*“. Můžeme totiž vyjít z dané formule s proměnnými a vytvořit instanci této formule, kde nahradíme proměnné příslušnými termy. Z věty o instancích potom plyne platnost takto upravené formule.

Nyní uvedeme větu, která je obdobou věty o ekvivalenci.

Věta o rovnosti 2.4.5. Nechť $t_1,\ldots,t_n$ a $s_1,\ldots,s_n$ jsou termy takové, že pro $\forall i \in \{1,\ldots, n\}$ platí $T \vdash t_i = s_i$

(i) Je-li *t* term a *s* term, který vznikne z *t* záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom:

$T \vdash t = s$

(ii) Je-li A formule a A' formule, která vznikne z A záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom:

$T \vdash A \equiv A'$

Důkaz. (i) Indukci podle složitosti termu t:

- Je-li t zaměněný term t_i, potom s je s_i a rovnost $T \vdash t = s$ plyne ihned z předpokladu $T \vdash t_i = s_i$.
- Je-li t nezaměněná proměnná, potom s je t a rovnost $T \vdash t = s$ plyne ihned z axiomu identity.
- Je-li t nezaměněná funkce $f(r_1, \ldots, r_k)$, potom s je $f(r'_1, \ldots, r'_k)$, přičemž z indukčního předpokladu máme $T \vdash r_i = r'_1$ pro $\forall i \in \{1, \ldots, k\}$. Vyjdeme z axiomu rovnosti pro funkce:

$\vdash r_1 = r'_1 \supset \ldots \supset r_k = r'_k \supset f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$

Formule $T \vdash f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$ neboli $T \vdash t = s$ zbude po k-násobné aplikaci pravidla (MP) na indukční předpoklad.

(iii) Protože se termy vyskytují pouze v atomických formulích, stačí, když dokážeme, že všechny atomické podformule formule A ve tvaru $p(r_1, \ldots, r_k)$, jsou ekvivalentní svým transformovaným variantám $p(r'_1, \ldots, r'_k)$. Tvrzení věty potom vyplyne z věty o ekvivalenci.

Z části (i) této věty víme, že pro $\forall i \in \{1, \ldots, k\}$, je $\vdash r_i = r'_i$. Použijeme-li axiom rovnosti pro predikáty

$\vdash r_1 = r'_1 \supset \ldots \supset r_k = r'_k \supset p(r_1, \ldots, r_k) \supset p(r'_1, \ldots, r'_k)$ (1)

dostaneme implikaci $p(r_1, \ldots, r_k) \supset p(r'_1, \ldots, r'_k)$ použitím k pravidel (MP).

Opačnou implikaci odvodíme podobně. Ve formuli (1) nejprve prohodíme čárkované a nečárkované symboly pro termy. Protože použitím symetrie rovnosti (*tvrzení 2.4.2.*) a pravidla (MP) snadno dojdeme od věty $\vdash r_i = r'_i$ k větě $\vdash r'_i = r_i$, dostaneme opačnou implikaci opět k-násobným (MP).

Následující důsledek je pouze jinou formou věty o rovnosti.

Důsledek 2.4.6. Jsou-li $t_1,\ldots..,\ t_n$ a $s_1,\ldots.,\ s_n$ termy, term s vznikne z termu t záměnou některých výskytů termů t_i odpovídajícími termy s_i a formule A' vznikne z formule A taktéž záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom platí:

(i) $\vdash t_1 = s_1 \supset \ldots. \supset t_n = s_n \supset t = s$

(ii) $\vdash t_1 = s_1 \supset \ldots. \supset t_n = s_n \supset (A \equiv A')$

Důkaz. Termy t a s, lze zapsat jako instance jediného termu r, který má na místě nahrazovaných podtermů proměnnou, pro každý různý podterm jednu novou (budiž to $z_1,\ldots.,z_n$). Potom:

$t \equiv r_{z1},\ldots.,_{zn}[t_1,\ldots.,t_n]$ $\qquad$ $s \equiv r_{z1},\ldots.,_{zn}[s_1,\ldots.,s_n]$ (1)

Stejně lze zapsat i formule A a A' pro nějakou formuli B jako:

$A \equiv B_{z1},\ldots.,_{zn}[t_1,\ldots..,t_n]$ $\qquad$ $A' \equiv B_{z1},\ldots.,_{zn}[s_1,\ldots..,s_n]$ (2)

Mějme nové konstanty $c_1,\ldots..,c_n$ a $d_1,\ldots..,d_n$. Budiž T množina formulí:

$T = \{c_1 = d_1, c_2 = d_2,\ldots.., c_n = d_n\}$

Potom jistě pro $\forall i \in \{1,\ldots.., n\}$ platí $T \vdash c_i = d_i$ a z věty o rovnosti máme:

$T \vdash r_{z1},\ldots.,_{zn}[c_1,\ldots..,c_n] = r_{z1},\ldots.,_{zn}[d_1,\ldots..,d_n]$

$T \vdash B_{z1},\ldots.,_{zn}[c_1,\ldots..,c_n] \equiv B_{z1},\ldots.,_{zn}[d_1,\ldots..,d_n]$

Protože je každá formule z T uzavřena, máme větou o dedukci:

$\vdash c_1 = d_1 \supset \ldots \supset c_n = d_n \supset r_{z1},\ldots.,_{zn}[c_1,\ldots..,c_n] = r_{z1},\ldots.,_{zn}[d_1,\ldots..,d_n]$

$\vdash c_1 = d_1 \supset \ldots \supset c_n = d_n \supset (B_{z1},\ldots.,_{zn}[c_1,\ldots..,c_n] \equiv B_{z1},\ldots.,_{zn}[d_1,\ldots..,d_n])$

Dále větou o konstantách získáme pro nové proměnné x_i a y_i:

$\vdash x_1 = y_1 \supset \ldots \supset x_n = y_n \supset r_{z1},\ldots.,_{zn}[x_1,\ldots..,x_n] = r_{z1},\ldots.,_{zn}[y_1,\ldots..,y_n]$

$\vdash x_1 = y_1 \supset : : : \supset x_n = y_n \supset (B_{z1},\ldots.,_{zn}[x_1,\ldots..,x_n] \equiv B_{z1},\ldots.,_{zn}[y_1,\ldots..,y_n])$

Dokazované formule vyplynou z těchto větou o instancích (proměnné x_i a y_i nahradíme termy t_i a s_i a přepisem podle (1) a (2)).

Tvrzení 2.4.7. Nechť A je formule, t term a x proměnná neobsažena v termu t. Potom:

(i) $\vdash Ax[t] \equiv (\forall x)(x = t \supset A)$

(ii) $\vdash Ax[t] \equiv (\exists x)(x = t \,\&\, A)$

Důkaz. (i) Zvlášť každou implikaci:

(1)	$\vdash (\forall x)(x = t \supset A) \supset (t = t \supset Ax[t])$	(AS)
(2)	$\vdash t = t \supset (\forall x)(x = t \supset A) \supset Ax[t]$	(ZP, MP)
(3)	$\vdash (\forall x)(x = t \supset A) \supset Ax[t]$	(R1, MP)
(4)	$\vdash x = t \supset (A \equiv Ax[t])$	(důsledek 2.4.6)
(5)	$\vdash Ax[t] \supset (x = t \supset A)$	(prostředky VL)
(6)	$\vdash Ax[t] \supset (\forall x)(x = t \supset A)$	(Z∀)

Krok (6) můžeme provést proto, že term t podle předpokladu neobsahuje proměnnou x a formule $Ax[t]$ ji tedy nemá volnou. Krok (5) plyne z věty výrokové logiky:

$A \supset (B \equiv C) \vdash A \supset (B \equiv C)$	(DP)
$A \supset (B \equiv C) \vdash A \supset (C \supset B)$	(VD, KI, VD)
$A \supset (B \equiv C) \vdash C \supset (A \supset B)$	(ZP, MP)
$\vdash [A \supset (B \equiv C)] \supset [C \supset (A \supset B)]$	(VD)

(ii) V zásadě podobně:

$\vdash [(A \supset (B \supset C))] \equiv [(A \wedge B) \supset C]$

(1) $\vdash (t = t \,\&\, Ax[t]) \supset (\exists x)(x = t \,\&\, A)$ (PS)
(2) $\vdash t = t \supset Ax[t] \supset (\exists x)(x = t \,\&\, A)$ (pomocí (1))
(3) $\vdash Ax[t] \supset (\exists x)(x = t \,\&\, A)$ (R1, MP)
(4) $\vdash x = t \supset (A \equiv Ax[t])$ (důsledek 2.4.6)
(5) $\vdash (x = t \wedge A) \supset Ax[t]$ (pomocí (1))
(6) $\vdash (\exists x)(x = t \wedge A) \supset Ax[t]$ (Z∃)

Příklad

Pro demonstraci ještě přidávám jednoduchý příklad.

Výchozí formule: $\exists x\, (f(g(x)) = x) \supset \exists y\, (g(f(y)) = y)$

1. $\exists x\, (f(g(x)) = x)$	Premisa
2. $f(g(c)) = c$	1, E∃

3. $(f(g(c)) = c) \supset g(f(g(c)) = g(c)$	ZI, kde t = $f(g(c))$
4. $g(f(g(c)) = g(c)$	2, 3, MP
5. $\exists y(g(f(y)) = y)$	4, Z$\exists$, kde t = g(c)
QED	1–5, ZI.

2.5 Monadická PL

Logika s pouze jednomístnými (unárními) predikáty. Monadická predikátová logika je fragment predikátového kalkulu, ve kterém jsou všechny predikátové symboly monadické (to znamená, že obsahují pouze jeden argument), a neobsahují žádné funkční predikáty. Všechny atomické formule mají tvar $P(x)$, kde P je predikát a x je předmětová (individuová) proměnná.

V zásadě se jedná o predikátové symboly s aritou rovno 1. Predikátová logika prvního řádu je obecně nerozhodnutelná. Nicméně monadická predikátová logika (bez rovnosti i s rovností), je speciální případ, ve kterém je problém logické pravdivosti formulí rozhodnutelný.

Příklad:

Nikdo, kdo trpí klaustrofobií nemůže pracovat jako liftboy.
Všichni horolezci trpí klaustrofobií.
———————————
Proto žádný horolezec nemůže pracovat jako liftboy.

Formalizace:
$\forall x[K(x) \supset \neg L(x)] \Rightarrow \forall x[\neg K(x) \vee \neg L(x)]$
$\forall x[H(x) \supset K(x)] \Rightarrow \forall x[\neg H(x) \vee K(x)]$
———————————
$\forall x[H(x) \supset \neg L(x)] \Leftrightarrow^{\neg} \exists x\,[H(x) \wedge L(x)]$

Rezoluce
1. $\neg K(x) \vee \neg L(x)$
2. $\neg H(x_1) \vee K(x_1)$
3. H(a)
4. L(a)

———————

5. $\neg K(a)$	1, 4	x/a
6. K(a)	2, 3	x_1/a
7. #spor	5, 6	

Došli jsme ke sporu. Původní formule je tedy tautologie.

2.6 Rezoluční metoda

Jelikož se tato diplomová práce samozřejmě neobejde bez příkladů, je nutné definovat alespoň jednu důkazovou metodu, na které budu příklady demonstrovat. Vybral jsem si rezoluční metodu. Níže jsou základní informace o rezoluční metodě.

Rezoluční metodu lze aplikovat pouze na formule speciálního tvaru, v tzv. klauzulární (Skolemově) formě. Nejprve proto ukážeme, že každou formuli je možno převést do klauzulární formy tak, že výsledná formule je splnitelná, právě když výchozí formule je splnitelná.

- Komplikovanější je procedura převedení formule na klauzulární tvar. Oproti výrokové logice obsahuje navíc:
  - převod formule na prenexní tvar,
  - eliminaci kvantifikátorů z formule.
- Složitější je tvar rezolučního odvozovacího pravidla. Jeho použití vyžaduje simultánní úpravu literálů, tzv. unifikaci.

Prenexní normální forma

Formule A predikátové logiky je v ***prenexním tvaru***, má-li podobu:
$Q_1x_1\ Q_2x_2...Q_nx_n\ B$, kde

- $n \geq 0$ a pro každé $i = 1, 2,...,n$ je Q_i buď všeobecný kvantifikátor $\forall$, nebo existenční $\exists$,
- $x_1, x_2,...,x_n$ jsou navzájem různé individuové proměnné,
- B je formule utvořená z elementárních formulí pouze užitím výrokových funktorů $\neg, \wedge, \vee$.

Výraz $Q_1x_1\ Q_2x_2...Q_nx_n$ se nazývá ***prefix (charakteristika)*** a B ***otevřeným jádrem (maticí)*** formule A v prenexním tvaru.

Každou formuli lze přepsat do prenexního tvaru, tj. ke každé formuli predikátové logiky A existuje formule A* v prenexním tvaru, která je s formulí A ekvivalentní (tj. $A \Leftrightarrow A^*$).

Převod formule do prenexního tvaru:

(1) Eliminace funktorů $\supset$ a $\equiv$. Toho lze dosáhnout užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$$A \supset B \Leftrightarrow \neg A \vee B,$$
$$A \equiv B \Leftrightarrow (A \supset B) \wedge (B \supset A) \Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A).$$

(2) Převedení formule na tvar s čistými proměnnými.

a) Použijeme následující ekvivalence (náhrady levé strany pravou):
$(\forall x A \wedge \forall x B) \Leftrightarrow \forall x\,(A \wedge B)$ $\quad$ $(\exists x A \vee \exists x B) \Leftrightarrow \exists x\,(A \vee B)$

b) Přejmenování vázaných proměnných tak, aby žádná proměnná nebyla ve formuli současně volná i vázaná a tak, aby všechny vázané proměnné byly navzájem různé. To platí nejenom pro celou formuli, ale i pro každou její podformuli.

(3) Vypuštění nadbytečných kvantifikátorů, tj. kvantifikátorů, jejichž oblast působnosti neobsahuje žádný výskyt kvantifikované proměnné.

(4) Přenesení všech výskytů funktoru negace bezprostředně před elementární formule. Toho lze dosáhnout opakovaným užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$\neg\neg A \Leftrightarrow A$,
$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$,
$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$,
$\neg\forall x\, A(x) \Leftrightarrow \exists x\, \neg A(x)$,
$\neg\exists x\, A(x) \Leftrightarrow \forall x\, \neg A(x)$.

(5) Přenesení všech kvantifikátorů na začátek formule. Toho lze dosáhnout opakovaným užitím následujících ekvivalencí (náhrady jejich levé strany pravou stranou):

$\forall x A \wedge B \Leftrightarrow \forall x\, (A \wedge B)$	$\exists x A \vee B \Leftrightarrow \exists x\, (A \vee B)$	B neobsahuje volnou x
$A \wedge \forall x B \Leftrightarrow \forall x\, (A \wedge B)$	$A \vee \exists x B \Leftrightarrow \exists x\, (A \vee B)$	A neobsahuje volnou x
$\exists x A \wedge B \Leftrightarrow \exists x\, (A \wedge B)$	$\forall x A \vee B \Leftrightarrow \forall x\, (A \vee B)$	B neobsahuje volnou x
$A \wedge \exists x B \Leftrightarrow \exists x\, (A \wedge B)$	$A \vee \forall x B \Leftrightarrow \forall x\, (A \vee B)$	A neobsahuje volnou x

Příklad:

Následující příklad demonstruje převod formule z prvního řádku na její prenexní tvar:

1.	$\forall x\, [p(x) \wedge \forall y \exists x\, (\neg q(x,y) \supset \forall z\, r(a,x,y))]$	(*výchozí formule*)
2.	$\forall x\, [p(x) \wedge \forall y \exists x\, (q(x,y) \vee \forall z\, r(a,x,y))]$	(*eliminace* $\supset$)
3.	$\forall x\, [p(x) \wedge \forall y \exists t\, (q(t,y) \vee \forall z\, r(a,t,y))]$	(*přejmenování proměnné*)
4.	$\forall x\, [p(x) \wedge \forall y \exists t\, (q(t,y) \vee r(a,t,y))]$	(*vypuštění nadbytečného kvantifikátoru*)
5.	$\forall x \forall y\, [p(x) \wedge \exists t\, (q(t,y) \vee r(a,t,y))]$	(*přesun kvantifikátoru doleva*)
6.	$\forall x \forall y \exists t\, [p(x) \wedge (q(t,y) \vee r(a,t,y))]$	(*přesun kvantifikátoru doleva*)

Pozn.: prenexní tvar formule není určen jednoznačně. Konečná podoba prenexní formule závisí na pořadí provádění úprav a na způsobu přejmenování vázaných proměnných. Všechny prenexní tvary jsou však ekvivalentní.

Skolemova klauzulární forma

Formule A predikátové logiky je ve Skolemově kaluzulární formě, je-li ***prenexním tvaru*** jehož prefix obsahuje pouze všeobecné kvantifikátory a matice je konjunkce klauzulí, kde každá klauzule je disjunkce literálů. Literál je atomická formule nebo její negace.

Skolem

Každá formule A může být převedena na formuli A^S v *klauzulární* (Skolemově) *formě* takovou, že A je splnitelná, právě když A^S je splnitelná.

Krok 1. Utvoření existenčního uzávěru formule A. (Zachovává splnitelnost.)

Krok 2. Eliminace nadbytečných kvantifikátorů. (Ekvivalentní krok.)
Z formule A vypustíme všechny kvantifikátory $\forall x_i$, $\exists x_i$, v jejichž rozsahu se nevyskytuje proměnná x_i.

Krok 3. Přejmenování proměnných. (Ekvivalentní krok.)
Přejmenujeme všechny proměnné, které jsou v A kvantifikovány více než jednou tak, aby všechny kvantifikátory měly navzájem různé proměnné.

Krok 4. Eliminace spojek $\supset$, $\equiv$ podle těchto vztahů (Ekvivalentní krok.):
$(A \supset B) \Leftrightarrow (\neg A \vee B)$, $(A \equiv B) \Leftrightarrow (\neg A \vee B) \wedge (\neg B \vee A)$

Krok 5. Přesun spojek $\neg$ *dovnitř.* (Ekvivalentní krok.)

Krok 6. Přesun kvantifikátorů doprava. (Ekvivalentní krok.)
Provádíme náhrady podle těchto ekvivalencí (Q je kvantifikátor $\forall$ nebo $\exists$; © je symbol $\wedge$ nebo $\vee$; A, B neobsahují volnou proměnnou x):
$Qx\ (A \copyright B(x)) \Leftrightarrow A \copyright Qx\ B(x)$, $Qx\ (A(x) \copyright B) \Leftrightarrow Qx\ A(x) \copyright B$

Krok 7. Eliminace existenčních kvantifikátorů (Zachovává splnitelnost.)
Provádíme postupně ***Skolemizaci podformulí*** $Qx\ B(x)$, $Qx\ A(x)$, které jsme obdrželi v předchozím kroku 6, tedy náhradu existenčně kvantifikovaných formulí formulemi bez existenčního kvantifikátoru takto:

$\exists x A(x)$ převedeme na A(a), kde a je nová, v jazyce dosud nepoužitá konstanta, pokud proměnná x není v dosahu žádného všeobecného kvantifikátoru. $\forall y_1 \ldots y_n\ \exists x A(x, y_1, \ldots, y_n)$ převedeme na $\forall y_1 \ldots y_n\ A(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$, kde f je nový n-ární funkční symbol.

Krok 8. Přesun všeobecných kvantifikátorů doleva. (Ekvivalentní krok, neboť jsme již provedli krok 3. a platí ekvivalence dle 6.)

Krok 9. Použití distributivních zákonů. (Ekvivalentní krok.)
Provedeme postupné náhrady vlevo formulemi vpravo

$(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$, $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

Příklad převodu formule na Skolemovu formu:

Výchozí formule: $\forall x \exists y \forall z \exists v [P(z,y) \wedge Q(x,y)]$

1. $\forall x \exists y \forall z \exists v [P(z,y) \wedge Q(x,y)] \Leftrightarrow$ (2. *Eliminace nadbytečných kvantifikátorů*)
2. $\forall x \exists y \forall z [P(z,y) \wedge Q(x,y)] \Leftrightarrow$ (6. *Přesun kvantifikátorů doprava*)
3. $\exists y [\forall z P(z,y) \wedge \forall x\ Q(x,y)] \Rightarrow$ (7. *Eliminace existenčních kvantifikátorů*)
4. $\forall z P(z,a) \wedge \forall x Q(x,a) \Rightarrow$ (8. *Přesun kvantifikátorů doleva*)
5. $\forall z \forall x P(z,a) \wedge Q(x,a)$ = Formule ve Skolemově formě

2.7 Přirozená dedukce

Metoda přirozené dedukce predikátové logiky je zobecněním metody přirozené dedukce výrokové logiky. Od této metody se liší pouze tím, že pracuje s obecnějším jazykem predikátové logiky a v souvislosti s tím používá rozšířenou množinu výchozích dedukčních pravidel

Definice

Výchozími (nedokazovanými, primárními) dedukčními pravidly jsou všechna dedukční pravidla uvedená níže pro práci s výrokovými funktory, tj.:

Zavedení konjunkce:	$A, B \vdash A \wedge B$	ZK	
Eliminace konjunkce:	$A \wedge B \vdash A, B$	EK	
Zavedení disjunkce:	$A \vdash A \vee B$ nebo $B \vdash A \vee B$	ZD	
Eliminace disjunkce:	$A \vee B, \neg A \vdash B$ nebo $A \vee B, \neg B \vdash A$	ED	
Zavedení implikace:	$B \vdash A \supset B$	ZI	
Eliminace implikace:	$A \supset B, A \vdash B$	EI	*modus ponens* **MP**
Zavedení ekvivalence:	$A \supset B, B \supset A \vdash A \equiv B$	ZE	
Eliminace ekvivalence:	$A \equiv B \vdash A \supset B, B \supset A$	EE	

a následující čtyři pravidla pro práci s kvantifikátory:

Zavedení obecného kvantifikátoru: $A(x) \vdash \forall x A(x)$ Z∀

Pravidlo lze použít pouze tehdy, jestliže formule $A(x)$ není odvozena z žádného předpokladu, který obsahuje x jako volnou proměnnou.

Eliminace obecného kvantifikátoru: $\forall x A(x) \vdash A(x/t)$ E∀

Formule $A(x/t)$ je výsledkem korektní substituce termu t za proměnnou x ve formuli $A(x)$, tedy term T musí být substituovatelný za x ve formuli A.

Zavedení existenčního kvantifikátoru: $A(x/t) \vdash \exists x A(x)$ Z∃

Eliminace existenčního kvantifikátoru: $\exists x A(x) \vdash A(x/c)$ E∃

Použijeme-li pravidlo E∃ pro různé formule A, musíme za proměnnou x substituovat vždy jinou konstantu c.

Obsahuje-li formule A, kromě kvantifikované proměnné x, ještě další volné proměnné, lze pravidlo eliminace existenčního kvantifikátoru formulovat obecněji takto:

$$\exists x\, A(x, y_1,...,y_n) \vdash A(\, x \,/\, f(y_1,...,y_n), y_1,...,y_n\,) \qquad E\exists$$

V tomto případě nelze za kvantifikovanou proměnnou x substituovat konstantu, ale funkci zbývajících (volných) proměnných. Použijeme-li pravidlo vícekrát pro různé formule A, musíme za proměnnou x substituovat vždy jinou funkci $f(y_1,...,y_n)$.

Příklad:

1) $\vdash \forall x\,[A(x) \supset B(x)] \supset [\forall x A(x) \supset \forall x B(x)]$

Důkaz:

1.	$\forall x\,[A(x) \supset B(x)]$	předpoklad	
2.	$\forall x A(x)$	předpoklad	
3.	$A(x) \supset B(x)$	E∀:1	
4.	$A(x)$	E∀:2	
5.	$B(x)$	MP:3,4	
6.	$\forall x B(x)$	Z∀:5	Q.E.D.

3 Rozhodnutelnost

Než přejdeme k samotným rozhodnutelným třídám (fragmentům) predikátové logiky prvního řadu, měli bychom si objasnit základní pojmy týkající se rozhodnutelnosti a nerozhodnutelnosti formulí v PL1.

O libovolné formuli můžeme prohlásit, že je rozhodnutelná pouze tehdy, existuje-li algoritmus, který dokáže vždy rozhodnout, že je daná formule tautologie, kontradikce či jen splnitelná. V opačném případě je formule nerozhodnutelná.

3.1 Logická pravdivost formulí PL1

Musím zdůraznit, že problém logické pravdivosti formulí je v predikátové logice - na rozdíl od výrokové logiky - nerozhodnutelný. To znamená, že neexistuje všeobecný algoritmus, který by vždy a s absolutní jistotou rozhodnul, zda předložená formule predikátové logiky je tautologie, kontradikce, anebo jen splnitelná.

Všeobecně tak můžeme říct, že predikátová logika je nerozhodnutelná. Avšak existují velké oblasti, kde tento problém je úspěšně zvládnutý (viz rozhodnutelné třídy).

3.2 Entscheidungsproblem

Do češtiny můžeme tento výraz přeložit jako rozhodovací problém. Entscheidungsproblem (rozhodovací problém), zformuloval v roce 1900 matematik David Hilbert. V něm se ptal, zda existuje mechanický proces, kterým je možné rozhodnout o pravdivosti libovolného matematického výroku. Pomocí Turingova stroje bylo později dokázáno, že to možné není.

Entscheidungsproblem spočíval ve snaze dokázat tvrzení, že ke každému matematickému výroku existuje ryze formální, mechanický proces, který by mu přiřadil pravdivostní hodnotu. Pokud by takový postup existoval, respektive byl nalezen, znamenalo by to, že matematika je naprosto soběstačný a úplný axiomatický systém, který je nezávislý na logice či jiné teorii. V roce 1935 až 1936 vytvořili Alan Turing a Alonzo Church - nezávisle na sobě - dvě různá řešení rozhodovacího problému, které byly vzájemně převeditelná a dokázaly, že takovýto algoritmus **nelze nalézt**.

V podstatě lze obě řešení považovat za rozvinutí Gödelovy teorie neúplnosti, ovšem technicky mnohem subtilnější. Church vymyslel λ-kalkul, jehož pomocí lze vyjádřit jakoukoli vyčíslitelnou funkci. Kalkul je velmi podobný funkcionálním programovacím jazykům. Přímo z něj vychází třeba dodnes používaný Lisp nebo Haskell. V rámci tohoto kalkulu Church převedl rozhodovací problém na hledání ekvivalence dvou výrazů pomocí univerzálního algoritmu a zjistil, že takový algoritmus neexistuje (Church 1936). Turing v publikaci „On Computable Numbers“, uvažoval podobným způsobem, ale jeho řešení je pro laika pochopitelnější, protože obsahuje velmi silnou metaforu pro průběh algoritmu, který přirovnává k mechanickému stroji provádějícímu jednodu-

ché, předprogramované úkony. Konkrétně nahradil složitou otázku: „Může stroj rozhodnout, zda je nějaké tvrzení dokazatelné?“ otázkou jednodušší: „Vytiskne někdy určitý stroj znak 0?“.

Tento Turingův idealizovaný stroj má konečný počet vnitřních stavů a obsahuje potenciálně 15 nekonečnou pásku rozdělenou do polí. Pole jsou označena symboly z konečné abecedy, ale pro fungování stroje je možné používat jen dva (např. 0 a 1). Stroj je také vybaven čtecí hlavou, která je schopna přečíst symbol na právě analyzovaném poli, a kromě toho umí symboly mazat a přepisovat. Reakce na čtené symboly je definována strojní neboli stavovou tabulkou; po přečtení symbolu se stroj podle předdefinovaných instrukcí rozhodne, má-li symbol smazat, přepsat nebo nechat být, a má-li se hlava posunout doleva, doprava nebo zůstat na tom samém poli. Chování stroje je tak zcela determinováno jeho konfigurací, tj. současným stavem a právě čteným symbolem. Popsaný stroj je schopen provádět vše, co dokáže jakýkoli reálně existující počítač. Ani pomocí takového stroje však nebylo a není možné dospět k obecnému algoritmu, který by definitivně vyřešil rozhodovací problém (Entscheidungsproblem)[35].

3.3 Nerozhodnutelnost

Věta (Churchova o nerozhodnutelnosti predikátové logiky)

Pokud spočetný jazyk L prvního řádu obsahuje alespoň jednu konstantu, alespoň jeden funkční symbol arity $k > 0$ a pro každé přirozené číslo spočetně mnoho predikátových symbolů, potom množina $\{\#A \mid A \text{ je uzavřená formule a } L \models A\}$ není rozhodnutelná.

Předchozí věta byla formulována k určitému důkazu. K nerozhodnutelnosti stačí daleko méně speciálních symbolů.

Věta (o nerozhodnosti predikátové logiky)

Nechť L je jazyk prvního řádu bez rovnosti a obsahuje alespoň dva binární predikáty. Potom je predikátová logika (jako teorie) s jazykem L nerozhodnutelná.

3.3.1 Tři axiomatizace aritmetiky

Robinsonova aritmetika Q.

Robinsonova aritmetika je neúplná a nerozhodnutelná. Je také značně slabší než Peanova aritmetika. Nicméně oproti Peanově aritmetice je Robinsonova aritmetika konečně axiomatizovaná (má konečný počet axiómů). Existuje 8 axiomů, které jsou uzávěry následujících formulí:

(Q1) $S(x) \neq 0$

(Q2) $S(x) = S(y) \supset x = y$

(Q3) $x \neq 0 \supset (\exists y)(x = S(y))$

(Q4) $x + 0 = x$

(Q5) $x + S(y) = S(x + y)$

(Q6) $x * 0 = 0$

(Q7) $x * S(y) = (x * y) + x$

(Q8) $x \leq y \equiv (\exists z)(z + x = y)$

Peanova aritmetika P (prvního řádu)

Peanova aritmetika je neúplná a také nerozhodnutelná. V matematické logice slouží k důkazu Gödelových vět o neúplnosti. Je také rozšířením Robinsonovi aritmetiky.

Peanova aritmetika má axiomy Q1 – Q8 (viz Robinsonova aritmetika) a navíc obsahuje schéma indukce. Pro každou formuli φ a každou proměnnou *x*, je následující formule axiom indukce:

$(\varphi(0) \wedge (\forall x)(\varphi(x) \supset \varphi(Sx))) \supset (\forall x)\varphi(x)$

Můžeme ukázat, že v Peanově aritmetice je dokazatelný axiom Q3, což znamená, že Peanova aritmetika je rozšířením Robinsonovy aritmetiky. Zároveň se dá ukázat, že axiomatika Peanovy aritmetiky je *rekurzivní*.

To znamená, že existuje algoritmus, který pro každou formuli PL1 rozhodne, zda je to axiom nebo není.

Úplná aritmetika.

Je-li *N* standardní model aritmetiky, pak má úplná aritmetika za axiomy všechny uzavřené formule, které jsou pravdivé v *N*.

$Th(N) = \{A \mid A \text{ je uzavřená formule } N \models A\}$

Tuto teorii můžeme také nazvat jako **pravdivá (přirozená) aritmetika**, protože je axiomatizovaná všemi formulemi, které jsou pravdivé ve standardním modelu *N*. Množině formulí Th(N), se říká teorie modelu *N*.

Máme tedy tři axiomatizace aritmetiky Q, P, Th(N), všechny v jazyku $L = \{0, S, +, *,\}$. Je tedy zřejmé, že

$Q \subseteq P \subseteq Th(N)$,

kde inkluze znamená rozšíření.

- Q má konečně mnoho axiomů, je tedy rekurzivně axiomatizovaná.
- P má spočetně axiomů - dá se tak ukázat, že kódy axiomů schématu indukce tvoří rekurzivní množinu. Spolu s dalšími konečně mnoha axiomy je P rekurzivně axiomatizovaná.
- Th(N) však není rekurzivně axiomatizovatelná.

Je-li T teorie s jazykem aritmetiky, můžeme definovat množinu kódů vět teorie T

$Thm(T) = \{ \#A \mid A \text{ je uzavřená formule, } T \vdash A \}$

Podle věty o uzávěru se tak stačí omezit na uzavřené formule.

Definice. Říkáme, že teorie T je rozhodnutelná, je-li množina Thm(T) (kódů) vět rekurzivní. Jinak je teorie nerozhodnutelná.

3.3.2 Nerozhodnutelné třídy

Následujících 16 prefixových tříd predikátové logiky prvního řádu je nerozhodnutelných. Tyto třídy jsou rozděleny podle toho, zda obsahují symbol rovnosti (viz predikátová logika s rovností) či funkční symboly.

A: Čistá predikátová logika (bez funkcí a bez rovnosti)

(1) $[\forall\exists\forall, (\omega, 1), (0)]$ (Kahr 1962)

(2) $[\forall^3\exists, (\omega, 1), (0)]$ (Suranyi 1959)

(3) $[\forall^*\exists, (0, 1), (0)]$ (Kalmar-Suranyi 1950)

(4) $[\forall\exists\forall^*, (0, 1), (0)]$ (Denton 1963)

(5) $[\forall\exists\forall\exists^*, (0, 1), (0)]$ (Gurevich 1966)

(6) $[\forall^3\exists^*, (0, 1), (0)]$ (Kalmar-Suranyi 1947)

(7) $[\forall\exists^*\forall, (0, 1), (0)]$ (Kostyrko-Genenz 1964)

(8) $[\exists^*\forall\exists\forall, (0, 1), (0)]$ (Suranyi 1959)

(9) $[\exists^*\forall^3\exists, (0, 1), (0)]$ (Suranyi 1959)

B: Třídy obsahující funkční symboly nebo rovnost

(10) $[\forall, (0), (2)]_=$ (Gurevich 1976)

(11) $[\forall, (0), (0, 1)]_=$ (Gurevich 1976)

(12) $[\forall^2, (0, 1), (1)]$ (Gurevich 1969)

(13) $[\forall^2, (1), (0, 1)]$ (Gurevich 1969)

(14) $[\forall^2\exists, (\omega, 1), (0)]_=$ (Goldfarb 1984)

(15) $[\exists^*\forall^2\exists, (0, 1), (0)]_=$ (Goldfarb 1984)

(16) $[\forall^2\exists^*, (0, 1), (0)]_=$ (Goldfarb 1984)

3.4 Parciální (částečná) rozhodnutelnost

A. Church v návaznosti na výsledky A. Turinga dokázal již v roce 1936, že neexistuje obecná rozhodovací procedura pro logickou pravdivost formule jazyka prvního řádu predikátové logiky. Přesněji, Churchova věta tvrdí, že problém logické pravdivosti formule je v predikátové logice pouze částečně (parciálně) rozhodnutelný. Což jiným slovy znamená, že existuje algoritmus, který v případě logicky pravdivé formule skončí kladnou odpovědí, v opačném případě dá buď odpověď zápornou, nebo se nezastaví (bude cyklit).

Můžeme tak říci, že pro predikátovou logiku lze vyvinout pouze kalkuly, které jsou jen parciálně rozhodnutelné – to znamená, pokud daná formule je tautologie, pak algoritmus po konečném počtu kroků odpoví ANO, v opačném případě nemusí vydat žádnou odpověď – může „cyklovat" či odpoví NE.

Důkaz logické pravdivosti můžeme demonstrovat na následujícím příkladu:

$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \supset \exists x Q(x)$ – Výchozí formule

Danou formuli nejprve znegujeme a postupně budeme uplatňovat algoritmus skolemizace. Pokud je znegovaná formule kontradikce, pak je původní tautologie.

Skolemizace:
$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \supset \exists x Q(x) \Leftrightarrow$ (*znegování formule*)

$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \wedge \forall x \neg Q(x) \Leftrightarrow$ (p*řejmenování proměnných*)

$[\forall x \exists y[P(x,y)] \wedge \forall x_1 [P(a,x_1) \supset Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Leftrightarrow$ (e*liminace spojek* $\supset, \equiv$)

$[\forall x \exists y[P(x,y)] \wedge \forall x_1 [\neg P(a,x_1) \vee Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Leftrightarrow$ (e*liminace existenčních kvantifikátorů*)

$[\forall x[P(x,f(x))] \wedge \forall x_1[\neg P(a,x_1) \vee Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Rightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall x_1 \forall x_2[P(x,f(x)) \wedge (\neg P(a,x_1) \vee Q(x_1)) \wedge \neg Q(x_2)]$

Sepíšeme si jednotlivé klausule pod sebe a budeme provádět unifikaci literálů tak, abychom postupně mohli uplatňovat rezoluční pravidlo.

Samotná rezoluce:
1. $P(x,f(x))$
2. $\neg P(a,x_1) \vee Q(x_1)$
3. $\neg Q(x_2)$
4. $\neg P(a,x_1)$ rezoluce 2, 3 x_2/x_1
5. #spor rezoluce 1, 4 $x_2/f(x)$ x/a

Došli jsme ke sporu, tím pádem můžeme říct, že původní formule je tautologií.

Obecná rezoluční metoda však pouze částečně rozhodnuje, zda je daná formule logicky pravdivá (problém je semidecidable), tzn. existuje algoritmus, který se zastaví pro každou logicky pravdivou, tj. v případě PL1 dokazatelnou formuli φ. Nicméně pro formule, které jsou pouze splnitelné, může algoritmus **pracovat věčně.**

Jako příklad formule, pro kterou bude algoritmus cyklovat, lze uvést tuto formuli:

$\forall x \exists y P(x,y) \wedge \forall x \neg P(x,x) \wedge \forall x \forall y \forall z([P(x,y) \wedge P(y,z)] \supset P(x,z))$

3.5 Rozhodnutelnost Presburgerovy aritmetiky

Presbergurova aritmetika je formální teorie prvního řádu, která obsahuje pouze funkční symbol pro sčítaní ne však násobení. Tedy tato aritmetika je teorie v jazyce L, který obsahuje konstantní symbol 0, unární funkční symbol S a binární funkční symbol +. Axiomy jsou následující:

(PR1) $0 \neq S(x)$

(PR2) $S(x) = S(y) \supset x = y$

(PR3) $x + 0 = x$

(PR4) $x + S(y) = S(x + y)$

(schéma indukce) $\varphi(0) \wedge (\forall x)(\varphi(x) \supset \varphi(S(x))) \supset (\forall x)(\varphi(x))$, pro všechny formule jazyka L.

Každá formule jazyka L je v Presburgerově aritmetice ekvivalentní nějaké formuli, která je v jednom z následujících tvarů:

$t = s$, $(\exists z)(t + z = s)$, $(\exists z)(t = s + nz)$,

kde n je *numerál*, jenž značí term, který vznikne n-násobnou aplikací funkčního symbolu S na konstantní symbol 0. Dále zde figurují termy s a t.

Presburgerova aritmetika je podstatně slabší než Peanova aritmetika, což je způsobeno právě absencí symbolu pro násobení. Nicméně - na rozdíl od Peanovy aritmetiky - existuje algoritmus, který může rozhodnout, zda daná sentence v Presbergurově aritmetice je pravdivá v zamýšleném modelu (sčítání na přirozených číslech) ve smyslu dokazatelná z axiomů této teorie.

Presburg také ukázal, že jeho aritmetika je bezesporná (neobsahuje kontradikce) a úplná (každé tvrzení může být buďto prokázáno nebo vyvráceno), což neplatí pro Peanovu aritmetiku v důsledku Gödelovi věty o neúplnosti.

Fischer a Rabin (1974) dokázali, že každý algoritmus, který rozhodne pravdivost tvrzení Presbergurovy aritmetiky, má dobu minimálně $2^{2^{cn}}$ (pro nějakou konstantu c, kde n je délka tvrzení). Je také známo, že tento problém je jeden z mála, který vyžaduje delší než polynomiální čas.

3.6 Rozhodnutelnost Σ-formulí

Další zajímavý pojem je *Σ-úplnost teorie Q*. Dokazujeme tak, že Q a žádná rozumná silnější teorie není úplná. Na druhé straně však existuje třída formulí (Σ-formule – jsou v úzkém vztahu k algoritmům) takových, že každý Σ-výrok pravdivý v **N** je dokazatelný v Q. Přitom z rekurzivní axiomatizovanosti teorie T plyne, že množina Gödelových čísel formulí dokazatelných v T je definovatelná v N jistou Σ-formulí, kterou označíme Dok(x). Tedy: Teorie T dokazuje φ právě když Dok(gn(φ)) je pravdivé v **N**. (gn(φ) je numerál, jehož významem je Gödelovo číslo formule φ).[12]

Σ-úplná teorie je například Robinsonova aritmetika, tzn. že pro každou *Σ-formuli* φ a přirozená čísla *k, n_1,....n_k* platí, že φ(n_1,….n_k) je dokazatelná Robinsonově aritmetice ≡ N |= φ[n_1,….n_k].

Formule φ je *Σ-formule*, která vznikla z otevřené formule opakovaným užitím konjunkce, disjunkce, omezené kvantifikace a (neomezené) existenční kvantifikace.

4 Rozhodnutelné podtřídy formulí PL1

V předcházející kapitole jsme si podrobněji rozebrali problém nerozhodnutelnosti logické pravdivosti formulí predikátové logiky. Nyní si ukážeme, že existuje řada podtříd (fragmentů), ve kterých je problém logické pravdivosti formule predikátové logiky prvního řádu rozhodnutelný.

V této kapitole vycházím především z výsledků, které mi poskytla kniha *The Classical Decision Problem* [2] od autorů: Egon Börger, Erich Gradel, Yuri Gurevich.

4.1 Historie

Studium rozhodnutelných tříd problému *Entscheidungsproblem* (rozhodovací problém – probráno v předešlé kapitole) začalo Löwenheimovou převratnou studií *Mathematische Annalen*, kde byla ustanovena rozhodnutelnost a vlastnost konečného modelu u monadického predikátového kalkulu (také včetně rovnosti).

Tatáž studie ukázala, že logika prvního řádu obsahuje axiomy nekonečna a dokázala, že problém platnosti může být u logiky prvního řádu redukován na problém platnosti čistého predikátového kalkulu (predikátový kalkul bez rovnosti a funkčních symbolů), který má pouze binární predikáty. Skolem a Behmann rozšířili výsledek Löwenheimovy rozhodnutelnosti na část logiky druhého řádu, v níž všechny predikáty, volné i vázané, jsou monadické.

První výsledky rozhodnutelnosti pro třídy formulí s nemonadickými predikáty byly důsledkem práce Bernayse a Schönfinkela v roce 1928 a týkaly se prefixových tříd $\exists^*\forall^*$ a $\forall\exists$ v čistém predikátovém kalkulu s relačními symboly libovolné arity. Ackermann rozšířil tyto druhé výsledky na třídu relačních sentencí $\exists^*\forall\exists^*$ s nejvýše jedním všeobecným kvantifikátorem. Další důkazy stejného výsledku dodal Skolem a Herbrand. Ramsey dokázal, že problém logické pravdivosti pro relační sentence $\exists^*\forall^*$ je rozhodnutelný rovněž v predikátovém kalkulu s rovností. Fakticky dokázal, že spektrum každé sentence $\exists^*\forall^*$ - bez funkčních symbolů - je buďto konečné nebo kokonečné. Aby toto dokázal, vyvinul slavnou kombinatorickou větu a zahájil to, co je dnes známé jako Ramseyho teorie, která stále zůstává velmi aktivním podoborem kombinatoriky.

V letech 1932 – 1934 Gödel, Kalmár a Schütte nezávisle na sobě objevili rozhodovací procedury pro třídu sentencí $\exists^*\forall^2\exists^*$ v čisté predikátové logice. Gödel a Schütte rovněž zavedli vlastnost konečného modelu u této třídy. Originální důkaz se opírá o geniální a velmi komplikovanou modelovou konstrukci. V roce 1984 nalezli Gurevich a Shelah jednodušší důkaz, který nahrazuje Gödelovu explicitní kombinatorickou konstrukci pravděpodobnostním argumentem.

Výsledky, že prefixové třídy $\forall^3\exists$ a $\forall\exists\forall$ v čisté predikátové logice jsou redukčními třídami - které byly později získané dvojicí Surányi, Kahr a Moore, Wang - ukázaly, že Bernays-Schönfinkelova třída $[\exists^*\forall^*]$ a Gödel-Kalmár-Schütteova třída $[\exists^*\forall^2\exists^*]$ jsou dvě maximální rozhodnutelné prefixové třídy v čisté predikátové logice, které jsou rozhodnutelné pro splnitelnost (a konečnou splnitelnost).

Na konci své studie Gödel bez odůvodnění tvrdí, že jeho metoda pro demonstraci vlastnosti konečného modelu pro třídu $\forall^2\exists^*$ je dostačující k tomu, aby ukázala stejný výsledek taktéž v přítomnosti rovnosti. Jenže v 60. letech 20. století byly objeveny ukázky dokazující, že Gödelovo kritérium není dostačující pro splnitelnost sentencí $\forall^2\exists^*$ obsahujících rovnost. V roce 1984 Goldfarb dokázal nerozhodnutelnost třídy $\forall^2\exists$, čímž dokončil klasifikace rozhodnutelných a nerozhodnutelných prefixových tříd obsahujících rovnost.

V predikátové logice s rovností (ale bez funkčních symbolů) tak sentence $\exists^*\forall\exists^*$ a sentence $\exists^*\forall^*$ tvoří maximální rozhodnutelné prefixové třídy.

Třídy formulí s funkčními symboly byly po dlouhou dobu vyřazeny z úvah. Až v roce 1954 na samém konci své knihy, fakticky na posledních čtyřech řádcích, navrhl Ackermann, aby byl prozkoumán rozhodovací problém u formulí s predikáty i funkcemi zároveň.

Nicméně toto studium nebylo zahájeno dříve než v 60. letech 20. století, kdy Löb a Gurevich dokázali, že logika prvního řádu s rovností a s pouze monadickými predikátovými a funkčními symboly (třída $[all, (\omega), (\omega)]_=$), má vlastnost konečného modelu.

Gurevich potom v sérii studií klasifikoval rozhodnutelné a nerozhodnutelné standardní třídy s funkčními symboly. Nejkomplikovanější případ v logice prvního řádu s rovností je třída sentencí $\exists^*\forall\exists^*$ s libovolnou slovní zásobou relačních a funkčních symbolů. Gurevich dokázal, že tato třída má vlastnost konečného modelu a je tudíž rozhodnutelná pro splnitelnost. Výsledek rozhodnutelnosti (ne však vlastnosti konečného modelu) rovněž vyplývá z faktu, že problém derivovatelnosti u třídy $[\exists^*\forall\exists^*, all, all]$ je rozhodnutelný. Tento fakt byl oznámen Orevkovem a dokázán Maslovem a Orevkovem, kteří citují Gurevichův důkaz (přijatý k publikaci v roce 1968, který byl ale publikován až v roce 1973). Jejich metoda je založena na teorii důkazů a je značně odlišná od metody Gurevichovy.

Sentence $\exists^*\forall\exists^*$ tak tvoří jedinečnou maximální rozhodnutelnou prefixovou třídu v logice prvního řádu, zatímco sentence $\forall^2$ tvoří třídu redukční (i s velmi omezenou slovní zásobou, jako např. unární relace a jedna binární funkce nebo binární relace a jedna unární funkce).

Pro „plnou“ logiku prvního řádu (s rovností, libovolnými funkcemi a s relačními symboly) je rozhodnutelná pouze existenční prefixová třída (kterou lze okamžitě zredukovat na propoziční případ). Gurevich fakticky prokázal, že třídy $[\forall, (0), (2)]_=$ a $[\forall, (0), (0, 1)]_=$ jsou redukčními třídami. Tímto nám zůstávají dvě maximální standardní třídy, z nichž obě obsahují axiomy nekonečna, a to konkrétně: Rabinova třída $[all, (\omega), (1)]_=$ a Shelahova třída $[\exists^*\forall\exists^*, all, (1)]_=$.

Studium výsledků komplexity u rozhodnutelných případů rozhodovacího problému má počátky v práci Lewise a Fürera, kteří určili horní a dolní hranice složitosti pro klasické řešitelné případy. Konkrétně dokázali, že Löwenheimova třída, Bernays-Schönfinkelova třída a Gödel-Kalmár-Schütteova třída mají nedeterministickou exponenciální časovou složitost a že Ackermannova třída má deterministickou exponenciální časovou složitost. Složitost Ackermannovy třídy $[\exists^*\forall\exists^*, all]_=$ s rovností určili Kolaitis a Vardi.

Grädel zkoumal složitost tříd s funkčními symboly. Konkrétně posílil Gurevichovy rozhodovací procedury u tříd $[\exists^*\forall\exists^*, all, all]$ a $[all, (\omega), (\omega)]$.

4.2 Rozhodnutelné třídy

V této a další kapitole si představíme kompletní popis standardních tříd, u nichž je problém splnitelnosti a problém konečné splnitelnosti rozhodnutelný. Rovněž se budeme zabývat komplexitou rozhodnutelných tříd a ve většině případů si rovněž představíme odpovídající horní a dolní meze složitosti. Navíc představíme klasifikaci tříd s vlastností konečného modelu.

Na začátek poznamenám, že existují třídy, jejichž problémy splnitelnosti a konečné splnitelnosti jsou rozhodnutelné z triviálních důvodů. Tyto třídy nebudu zahrnovat do našich budoucích úvah. Jde o (relační) třídy $[\Pi, s]$ či $[\Pi, s]_{=}$, kde Π a $s = (s_1, s_2, ...)$ jsou konečné v následujícím smyslu:

- $\Pi \in \{\exists, \forall\}^*$, tzn. že Π neobsahuje žádné případy výskytu $\exists^*$ nebo $\forall^*$ a definuje tak konečnou množinu prefixů.

- $s_i \neq \omega$ pro každé i a $s_i = 0$ u téměř konečně mnoho i; s tudíž definuje (až do přejmenování) konečnou slovní zásobu relačních symbolů.

Takové třídy nazýváme *esenciálně konečné,* neboť jejich formule jsou sestaveny z (dokud nejsou relační symboly a proměnné přejmenovány) konečné kolekce atomických formulí K. Nyní můžeme opravit jména proměnných a relačních symbolů a ustanovit nad K lineární uspořádání. Toto indukuje lineární uspořádání u formulí v konjunktivní normální formě sestavených z atomů kolekce K. Každou formuli v esenciálně konečné třídě lze efektivně zredukovat na ekvivalentní formuli, jejíž část bez kvantifikátorů je minimální (s ohledem na zvolené uspořádání) konjunktivní normální formou. Splnitelnost (a konečnou splnitelnost) esenciálně konečných tříd lze proto rozhodnout transformací daných formulí do takovéto normální formy, čímž se problém redukuje na konečný počet instancí, a následným vyhledáním odpovědi v tabulce. Je jasné, že tuto proceduru lze implementovat za použití pouze logaritmického pracovního prostoru. Tímto jsme dokázali následující:

Propozice. U každé esenciálně konečné třídy X jsou problémy Sat(X) a Fin-sat(X) rozhodnutelné v logaritmickém prostoru. V pokračování tudíž omezíme naši pozornost na standardní třídy $[\Pi, s, t]$ a $[\Pi, s, t]_{=}$, které splňují alespoň jednu z následujících podmínek:

- Π obsahuje instanci $\exists^*$ nebo $\forall^*$;

- $t = 0$;

- s není konečné.

Dokážeme, že všechny standardní třídy $[\Pi, s, t]$ nebo $[\Pi, s, t]_{=}$, které neobsahují žádnou z níže uvedených šestnácti konzervativních tříd, jsou rozhodnutelné.

Třídy s konečným prefixem:
– $[\forall\exists\forall, (\omega, 1), (0)]$ (Kahr 1962)
– $[\forall^3\exists, (\omega, 1), (0)]$ (Surányi 1959)

Třídy s prefixem ∀*:
– [∀*∃, (0, 1), (0)] (Kalmár-Surányi 1950)
– [∀∃∀*, (0, 1), (0)] (Denton 1963)

Třídy s prefixem ∃*:
– [∀∃∀∃*, (0, 1), (0)] (Gurevich 1966)
– [$\forall^3\exists$*, (0, 1), (0)] (Kalmár-Sur´anyi 1947)
– [∀∃*∀, (0, 1), (0)] (Kostyrko-Genenz 1964)
– [∃*∀∃∀, (0, 1), (0)] (Surányi 1959)
– [∃*$\forall^3\exists$, (0, 1), (0)] (Surányi 1959)

Třídy s rovností a funkčními symboly (Gurevich 1976):
– [∀, (0), (2)]$_=$
– [∀, (0), (0, 1)]$_=$

Třídy bez rovností a s funkčními symboly (Gurevich 1969):
– [$\forall^2$, (0, 1), (1)]
– [$\forall^2$, (1), (0, 1)]

Třídy s rovností bez funkčních symbolů (Goldfarb 1984):
– [$\forall^2\exists$, (ω, 1), (0)]$_=$
– [∃*$\forall^2\exists$, (0, 1), (0)]$_=$
– [$\forall^2\exists$*, (0, 1), (0)]$_=$

Fakticky si tak můžeme představit *sedm maximálních standardních tříd,* u nichž je splnitelnost (a konečná splnitelnost) rozhodnutelná. Jedná se o 5 tříd s vlastností konečného modelu a 2 třídy obsahující axiomy nekonečna.

B: třídy s vlastností konečného modelu
(1) [∃*∀*, all, (0)]$_=$ *(Ramsey 1930)*
(2) [∃*$\forall^2\exists$*, all, (0)] *(Godel 1932, Kalmár 1933, Schutte 1934)*
(3) [all, (ω), (ω)] *(Löb 1967, Gurevich 1969)*
(4) [∃*∀∃*, all, all] *(Gurevich 1973, Maslov-Orevkov 1972)*
(5) [∃*, all, all]$_=$ *(Gurevich 1976)*

B: třídy obsahující axiomy nekonečna
(6) [all, (ω), (1)]$_=$ *(Rabin 1969)*
(7) [∃*∀∃*, all, (1)]$_=$ *(Shelah 1977)*

Vlastnost konečného modelu vs. axiomy nekonečna

Otázka zdali má nějaká třída formulí vlastnost konečného modelu nebo zdali obsahuje axiomy nekonečna je zajímavá sama o sobě. Je tudíž žádoucí mít systém klasifikace tříd prefixových slovních zásob s ohledem na tuto otázku. Z Gurevichovy věty o klasifikovatelnosti vyplývá, že rovněž v tomto případě existuje konečná klasifikace.

V mnoha případech jsme viděli, že problém splnitelnosti (a konečný problém splnitelnosti) u třídy prefixové slovní zásoby je rozhodnutelný tehdy a pouze tehdy, když má vlastnost konečného modelu. Pokud je však ve formuli přítomna rovnost i funkční symboly, pak zde můžeme mít rozhodnutelné třídy s axiomy nekonečna.

Maximálními z nich jsou Rabinova třída $[all, (\omega), (1)]_{=}$ a Shelahova třída $[\exists^*\forall\exists^*, all, (1)]_{=}$. Měli bychom rovněž zmínit, že esenciálně konečné třídy - tj. třídy s konečným prefixem a konečným relačním slovníkem - nelze v tomto případě opomenout. Tyto třídy jsou triviální pro algoritmické otázky, jako je rozhodnutelnost problému splnitelnosti, ale mohou samozřejmě obsahovat axiomy nekonečna. Fakticky kterýkoliv konkrétní axiom nekonečna má konečnou slovní zásobu a konečný prefix. Každá relační redukční třída má tudíž konečné podtřídy s axiomy nekonečna.

Příklad: Sentence

$\varphi := \forall x\exists y\forall z(\neg Rxx \wedge Rxy \wedge (Ryz \supset Rxz))$

$\psi := \forall x\forall y\forall z\exists u(\neg Rxx \wedge Rxu \wedge (Rxy \wedge Ryz \supset Rxz))$

jsou axiomy nekonečna v konečných třídách $[\forall\exists\forall, (0, 1)]$ a $[\forall^3\exists, (0, 1)]$.

Klasifikaci si představíme skrze dva výroky. První dává seznam maximálních tříd s vlastností konečného modelu, druhý dává seznam všech minimálních tříd s axiomy nekonečna. Tyto dva seznamy zahrnují takřka všechny prefixové třídy slovních zásob.

Výše jsme krátce rozebrali historii rozhodnutelných tříd a nastínili rozdíl mezi axiomy nekonečna a vlastností konečného modelu. Nyní si rozebereme jednotlivé třídy podrobněji. Začneme třídami, s vlastností konečného modelu: Löb-Gurevichova třída, Bernays–Schönfinkelova třída, Gödel-Kalmár-Schütteova třída, Gurevich-Maslov-Orevkova třída a Gurevichova třída.

4.2.1 Rozhodnutelné třídy s vlastností konečného modelu

Předtím, než Church a Turing dokázali neřešitelnost problému *Entscheidungsproblem*, přišla řada matematiků s pozitivními výsledky pro konkrétní podpřípady. Nejslavnější jsou výsledky rozhodnutelnosti pro následující případy:

$[all, (\omega)]$	(Löwenheim 1915)
$[\exists^*\forall^*, all]$	(Bernays, Schöfinkel 1928)
$[\exists^*\forall\exists^*, all]$	(Ackermann 1928)
$[\exists^*\forall^2\exists^*, all]$	(Gödel 1932, Kalmár 1933, Schütte 1934)

Těmto třídám se často říká *klasické řešitelné případy* rozhodovacího problému. Kromě Löwenheimovi třídy se budeme zabývat i jejími rozšířeními s rovností (tak dostaneme třídu $[all,(\omega)]_{=}$) a unárními symboly funkcí (takto získáme Löb-Gurevichovu třídu $[all, (\omega), (\omega)]$ - jeden z maximálních řešitelných případů).

V sekci 4.2.1.3 se zabývám třídou relačních formulí $\exists^*\forall^*$ - Bernays-Schönfinkelovou třídou.

V sekci 4.2.1.2 se zabývám Gödel-Kalmár-Schüttovou třídou [$\exists^*\forall^2\exists^*$, *all*].

U této třídy si dokážeme vlastnost konečného modelu pravděpodobnostním přístupem podle Gurevicha a Shelaho, který dramatickým způsobem zjednodušuje nejtěžší část originálního Gödelova důkazu. Všechny tyto třídy mají nedeterministickou exponenciální časovou složitost.

4.2.1.1 Löb-Gurevichova třída

Löb-Gurevichova třída, je třída všech těch formulí, které obsahují pouze monadické predikátové symboly. Jedná se tak tedy o monadickou predikátovou logiku, u které je problém logické pravdivosti formulí rozhodnutelný.

Ještě než přistoupíme k samotnému důkazu, trochu upravíme terminologii. Třídy [*all,*(ω)] a [*all,*(ω)]$_=$ se nazývají *Löwenheimova třída* a *Löwenheimova třída s rovností*. Formule v těchto třídách se nazývají *relační monadické formule*. Expanzí Löwenheimovy třídy - s unárními funkčními symboly - dostáváme *plnou monadickou třídu* [*all,* (ω), (ω)], která se rovněž nazývá **Löb-Gurevichova třída**. Její prvky jsou monadické formule.

Dokážeme si, že plná monadická třída a Löwenheimova třída s rovností mají vlastnost konečného modelu, a fakticky ustanovíme meze u velikosti minimálních modelů monadických formulí, čímž dokážeme vlastnost konečného modelu, které nám dají dobré horní meze složitosti pro problémy splnitelnosti těchto tříd.

Test splnitelnosti formulí u Löwenheimovy třídy (s rovností) má složitost Ntime($2^{O}(n$ / log). U plné monadické třídy je složitost nepatrně vyšší: splnitelnost je rozhodnutelná v Ntime($2^{O}(n)$).

Rovněž dokážeme dolní meze složitosti. Dolní meze se fakticky vztahují na malé subfragmenty těchto tříd a konkrétně nám dávají dobrou dolní mez i pro Gödel-Kalmár-Schüttovu třídu.

Rozhodnutelnost a horní meze složitosti u monadické třídy
Prvně ustanovíme vlastnost malého modelu u Löwenheimovy třídy s rovností.

Propozice 4.2.1.1.1. *Nechť ψ je relační monadická formule s případnou rovností, s hodností kvantifikátorů q a s m predikáty. Pokud je ψ splnitelná, pak má model kardinality nanejvýš $q2^m$.*

Důkaz. Nechť $\mathfrak{A} = (A, P_1, \ldots, P_m) \models \psi$. S každým elementem $a \in A$ asociujeme 'barvu' $c(a) = c_1 \ldots c_m \in \{0, 1\}^m$, kde $c_i = 1$, právě tehdy, když $\mathfrak{A} \models P_i a$. Nechť $A_c \subseteq A$ je množinou elementů s barvou c. Pro každé $c \in \{0, 1\}^m$ zvolíme množinu $B_c \subseteq A_c$ takovou, že $B_c = A_c$, pokud $|A_c| \leq q$ a zároveň $|B_c| = q$, jestliže $|A_c| > q$. Nechť $\mathfrak{B}$ je potom indukovanou substrukturou $\mathfrak{A}$ s univerzem $B := \bigcup_{\in\{0,1\}^m} B_c$. Je zřejmé, že $|B| \leq q2^m$.

Lze tak snadno zpozorovat, že žádná formule s q proměnnými nerozlišuje mezi $\mathfrak{A}$ a $\mathfrak{B}$, jelikož $\mathfrak{A} \models \psi$ a ψ má hodnotu kvantifikátorů q, což má pak za následek, že $\mathfrak{B} \models \psi$.

Důsledek 4.2.1.1.2 (Löwenheim). *Problém splnitelnosti u relačních monadických formulí je rozhodnutelný.*

Na Löwenheimovu třídu *bez rovnosti* se vztahují o něco přísnější meze.

U plné monadické třídy získáváme o něco vyšší horní mez složitosti u velikosti struktur, který je potřeba zkontrolovat:

Propozice 4.2.1.1.3 (Grädel). *Každá splnitelná monadická formule délky n má model kardinality* $2^{O(n)}$.

Důkaz. Ukážeme si, že každou monadickou formuli ψ délky *n,* lze transformovat do formule $\varphi \in$ [*all,* (*n*), (0)], která je splnitelná nad těmi samými doménami jako ψ.

Nechť ψ je monadická formule, která obsahuje atom $P\ f\ t$ (kde P je monadický predikát, f funkční symbol a t term) a nechť Q je zároveň nějaký nový predikát, který se nevyskytuje v ψ. Pak ψ je splnitelná nad stejnými doménami, jako

$$\psi\ [P\ f\ t/Qt] \wedge \forall x(P\ f\ x \equiv Qx),$$

kde $\psi\ [P\ f\ t/Qt]$ se získá z ψ nahrazení všech atomů $P\ f\ t,$ za Qt (pro libovolné termy t). Opakované aplikování této transformace vytvoří formuli

$$\psi' := \alpha \wedge \forall x\beta,$$

kde α neobsahuje žádné funkční symboly a β je konjunkcí ekvivalencí formule $P\ f\ x \equiv Qx$. Nechť $f_1, \ldots f_m$ jsou funkční symboly v β. Všimněte si, že $\forall x\beta$ je Skolemova normální forma z formule $\forall x \exists y_1 \ldots . \exists y_m \beta\ [fix / y_i]$, která je čistě relační. Podle Skolemovy věty o normální formě vyplývá, že formule

$$\varphi := \alpha \wedge \forall x \exists y_1 \ldots \exists y_m \beta\ [f_i x / y_i]$$

je splnitelná nad stejnými doménami jako ψ' a tudíž i ψ. Je zřejmé, že φ obsahuje nanejvýš n predikátů.

Konkrétně tedy platí, že monadické formule mají vlastnost konečného modelu.

Důsledek 4.2.1.1.4 (Löb, Gurevich). Sat[*all,* (ω), (ω)] *je rozhodnutelná.*

Bližší analýza nám poskytne horní mez složitosti.

Propozice 4.2.1.1.5 (Lewis). *Problém, zda daná monadická formule délky n má modelovou velikost s, lze rozhodnout nedeterministicky v* $2^{O(n / \log n + \log s)}$ *krocích.*

Důkaz. Představíme si nedeterministickou proceduru, která poté co je jí poskytnuta monadická formule ψ a modelová velikost s, se prvně pokusí uhodnout strukturu velikosti s vhodné slovní zásoby a pak ověří eliminací kvantifikátorů, že tato struktura je modelem pro ψ. Hádání struktury spočívá v zapsání slova délky s, pro každou relaci a slova délky $s \log s$ pro každou funkci v ψ. K tomu je potřeba $O((n / \log n)s \log s)$ bitů.

Kvantifikátory jsou eliminovány v následujících krocích. Začni nejvnitřejším kvantifikátorem a předpokládej, že je existenční a že jej musíme eliminovat z podformule $\exists x\varphi$, kde φ je formule bez

kvantifikátorů. Transformuj φ do disjunktivní normální formy, vyměň existenční kvantifikátor za disjunkce a odděl atomy, které obsahují x od těch, které jsou závislé na jiných proměnných. Výsledkem je nějaká formule

$$\bigvee_{j=1}^{r}(\tilde{\varphi}_j \wedge \exists x \varphi_j(x)),$$

kde každé $\varphi_j(x)$, je konjunkcí literálu $\pm P\ f\ x$ (kde f je kompozicí nejvýš n funkčních symbolů). Všimněte si, že $r = 2^{O(n\ /\ log\ n)}$ a že každá subformule $\tilde{\varphi}_j \wedge \exists x \varphi_j(x)$ obsahuje nanejvýš $O(n\ /\ \log\ n)$ rozdílných atomů původní formule ψ. Můžeme tudíž vyhodnotit každou podformuli $\exists x \varphi_j(x)$ a nahradit ji hodnotou *pravda* nebo *nepravda* v čase $O(n^2 \log n \cdot s \log s)$. Eliminace jednoho kvantifikátoru tudíž vyžaduje čas $2^{O(n\ /\ log\ n + log\ s)}$.

Všeobecné kvantifikátory se eliminují duální procedurou s použitím konjunktivní normální formy namísto disjunktivní normální formy. Tato procedura se opakuje pro každý kvantifikátor. Všechny přechodné formule jsou konjunktivními nebo disjunktivními normálními formami atomů, které byly původně v ψ, takže stejné meze jako výše zůstávají i po eliminaci každého kvantifikátoru v ψ. Celá rozhodovací procedura tudíž vezme $2^{O(n\ /\ log\ n + log\ s)}$ kroků.

Příklady

Následně uvádím několik příkladů a protipříkladů, kdy formule bude, respektive nebude splňovat podmínky Löb-Gurevichovy třídy.

Příklad:

Formule: $\exists x F(x) \wedge \exists x G(x) \Rightarrow^{S} \exists x(F(x) \wedge G(x))$

Teorém 1: (Löwenheim-Skolem 1915)
Je-li S monadická sentence, která je splnitelná, pak S je pravdivá v některé interpretaci, jejíž ohodnocení obsahuje nanejvýš $2^k \cdot r$ členů (kde k, je počet monadických predikátů a r je počet proměnných).

Část 1: Důkaz rozhodnutelnosti monadické predikátové formule z teorému 1.
Část 2: Důkaz teorému 1

Část 1: Důkaz rozhodnutelnosti monadické predikátové formule z teorému 1.
1. Asociuj S se sentencí bez kvantifikátorů S^*. Tato sentence je splnitelná právě tehdy, je-li splnitelná sentence S.

i) Najdi podformuli H pro S. Například $S = \forall x F(x) \vee \exists y G(y)$ $H: F(x), G(y), \forall x F(x)\ldots$

ii) Induktivně asociuj H^* - která neobsahuje žádné kvantifikátory - s každou podformulí H, tehdy:

a) Jestliže H je atomická, $H^* = H$;

b) Jestliže H je složená pravdivostní funkce, H^*

c) Jestliže $H = \exists v F$, $H = F(a_1) \vee F(a_2) \vee \ldots \vee F(a_m)$ $m = 2^k \cdot r$

d) Jestliže $H = \forall vF$, $H = F(a_1) \wedge F(a_2) \wedge \ldots \wedge F(a_m)$

iii) S a S^* má stejnou pravdivostní hodnotu ve stejném výkladu

2. Nyní už je jednoduché rozhodnout logickou pravdivost S^*. Tím pádem můžeme říci, že sentence S, je rozhodnutelná.

Část 2: Důkaz teorému 1

Předpokládejme, že M je modelem S, jehož doménou je D

1. Pro každé d v D, nechť je $s(d) = \langle j_1,\ldots,j_k\rangle$, kde pro každé I mezi 1 a k, $j_i = 1$ nebo 0.
   Podle toho určíme M tak, že P_i je pravdivé nebo nepravdivé v d. $2k$ jako sled $s(d)$.
2. C je podobné d, právě tehdy, když $s(c)=s(d)$. Podobnost je v tomto případě relace ekvivalence. Každé d v D patří do unikátní třídy ekvivalence. Nanejvýš 2^k třídy ekvivalence.
3. Sestrojte model M^* z S, jehož doména má nejvýše $2^k \cdot r$ členů

   i) E tvoří jeden celek: vyberte z každé ekvivalentní třídy r členů; pokud je v třídě méně než r členů, vyberte všechny členy.

   ii) E obsahuje maximálně $2^k \cdot r$ členů

   iii) M^* je interpretace, jehož doménou je E, která stanoví, že v P_i je pravdivé c právě tehdy, když M stanoví, že v P_i je pravdivé jakékoliv c v E
4. $M(S)$ = pravda, nyní vidíme, že $M(S) = M^*(S)$

Příklad 2

$\forall x(P(x) \supset \neg Q(x)) \supset [\forall x(R(x) \supset (P(x)) \supset \forall x(R(x) \supset \neg Q(x))]$ – Výchozí formule

Tato formule jistě splňuje omezení Lob-Gurevichovy třídy. Ukážeme si tedy její důkazů; původní formuli znegujeme a následně provedeme rezoluci.

Důkaz sporem

$\forall x(P(x) \supset \neg Q(x)) \supset [\forall x(R(x) \supset (P(x)) \supset \forall x(R(x) \supset \neg Q(x))] \Leftrightarrow$ (*negace formule*)

$\neg[\forall x(P(x) \supset \neg Q(x)) \supset [\forall x(R(x) \supset (P(x)) \supset \forall x(R(x) \supset \neg Q(x))]] \Leftrightarrow$ (*přesun negace dovnitř*)

$\forall x(P(x) \supset \neg Q(x)) \wedge \forall x(R(x) \supset (P(x)) \wedge \neg\forall x(R(x) \supset \neg Q(x)) \Leftrightarrow$ (*přesun negace dovnitř*)

$\forall x(P(x) \supset \neg Q(x)) \wedge \forall x(R(x) \supset (P(x)) \wedge \exists x(R(x) \wedge Q(x)) \Leftrightarrow$ (*přejmenování proměn.*, *eliminace* $\supset$)

$\forall x(\neg P(x) \vee \neg Q(x)) \wedge \forall y(\neg R(y) \vee (P(y)) \wedge \exists z(R(z) \wedge Q(z)) \Rightarrow$(*eliminace* $\exists$*, přesun kvant. doleva*)

$\forall x\forall y(\neg P(x) \vee \neg Q(x)) \wedge (\neg R(y) \vee (P(y)) \wedge (R(a) \wedge Q(a))$

Rezoluce

1. $\neg P(x) \vee \neg Q(x)$
2. $\neg R(y) \vee (P(y)$
3. $R(a)$
4. $Q(a)$

5. $\neg P(a)$ rezoluce 1, 4 x/a
6. $\neg R(a)$ rezoluce 2, 5 y/a
7. #spor rezoluce 3, 6

Můžeme říct, že tato formule je logicky pravdivá, jelikož jsme došli ke sporu a výchozí formule splňuje omezení této třídy.

Pro ukázku dále přidávám několik příkladů formulí, které nesplňují podmínky této podtřídy, tudíž nejsou rozhodnutelné.

Protipříklad

$\forall x[[\neg P(x) \vee Q(x, h(x)) \wedge \neg P(f(a))]$ – Výchozí formule

U této formule už nyní můžeme prohlásit, že není rozhodnutelná. Nesplňuje podmínky této podtřídy – neobsahuje pouze monadické predikáty. Nicméně ukážeme si její důkaz.

Původní formuli znegujeme a budeme se snažit nalézt spor. Pokud je znegovaná formule kontradikce, pak je původní tautologie.

Skolemizace
$\forall x[[\neg P(x) \vee Q(x, h(x)) \wedge \neg P(f(a))] \Leftrightarrow$ (*negace formule*)

$\exists x[[P(x) \wedge \neg Q(x, h(x)) \vee P(f(a))] \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$[[P(b) \wedge \neg Q(b, h(b)) \vee P(f(a))] \Leftrightarrow$ (*distributivní zákony*)

$[[(P(b) \vee P(f(a))) \wedge (\neg Q(b, h(b)) \vee P(f(a)))]$

Rezoluce
1. $P(b) \vee P(f(a))$
2. $\neg Q(b, h(b)) \vee P(f(a))$
3.

Nedošli jsme ke sporu, tudíž původní formule není tautologie.

Protipříklad 2

$\exists xQ(x) \supset [\forall x(P(x) \vee Q(x)) \supset \forall x \exists y T(x, y)]$ – Výchozí formule

Tato formule opět obsahuje i jiné než jen monadické predikáty. Tudíž nesplňuje podmínky této podtřídy.

Skolemizace
$\exists xQ(x) \supset [\forall x(P(x) \vee Q(x)) \supset \forall x \exists y\ T(x, y)] \Leftrightarrow$ (*negace formule*)

$\neg(\exists xQ(x) \supset [\forall x(P(x) \vee Q(x)) \supset \forall x \exists y\ T(x, y)]) \Leftrightarrow$ (*přejmenování proměnných*)

$\neg(\exists x Q(x) \supset [\forall x_1(P(x_1) \vee Q(x_1)) \supset \forall x_2 \exists y\, T(x_2, y)]) \Leftrightarrow$ (*eliminace implikace*)

$\neg\, (\forall x \neg Q(x) \vee [\exists x_1(\neg P(x_1) \wedge \neg Q(x_1)) \vee \forall x_2 \exists y\, T(x_2, y)]) \Leftrightarrow$ (*přesun negace dovnitř*)

$(\exists x Q(x) \wedge [\forall x_1(P(x_1) \vee Q(x_1)) \wedge \exists x_2 \forall y\, \neg T(x_2, y)]) \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$(Q(a) \wedge [\forall x_1(P(x_1) \vee Q(x_1)) \wedge \forall y\, \neg T(b, y)]) \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x_1 \forall y (Q(a) \wedge (P(x_1) \vee Q(x_1)) \wedge \neg T(b, y))$

Rezoluce
1. $Q(a)$
2. $P(x_1) \vee Q(x_1)$
3. $\neg T(b, y)$
4.

Nedošli jsme ke sporu; nelze dále unifikovat, proto původní formule není tautologie.

4.2.1.2 Gödel-Kalmár-Schütteova třída

Gödel-Kalmár-Schütteova třída je třída všech těch formulí, které v prenexní normální formě mají prefix ve tvaru $\exists^* \forall^2 \exists^*$ a formule dále neobsahuje žádné další kvantifikátory a žádné funkční symboly.

$\exists x_1 \cdots \exists x_n \forall x_1 \forall y_2 \exists x_1 \cdots \exists x_m\, \varphi$

Důkaz pravdivosti logických formulí je kompletně analogický důkazu v předchozí třídě. V něm jsme uvedli, že $m = O(n / \log n)$ existenčně kvantifikovaných konstant, které reprezentovaly m cifer užitých v m-ární notaci čísel až po m^m. Zde máme konstanty pouze dvě a používáme je k reprezentaci čísel až do 2^m v binární notaci.

Gödel-Kalmár-Schütteova třída: Pravděpodobnostní důkaz

V této sekci si ukazujeme, že problém splnitelnosti u Gödel-Kalmár-Schütteovy třídy [$\exists^* \forall^2 \exists^*$, *all*] je rozhodnutelný a že je fakticky obsažen v třídě složitosti NTIME $2^{O(n / \log n)}$.

Z expozičních důvodů nejdříve uvážíme případ formulí bez existenčních kvantifikátorů, tzn. prefixovou třídu [$\forall^2 \exists^*$].

Výrok 4.2.1.2.1 (Gödel, Schütte). *Třída* [$\forall^2 \exists^*$, *all*] *má vlastnost konečného modelu*

Tento výrok si dokážeme postupem podle Gödelovy obecné strategie [48]: prvně zformulujeme *nezbytné kritérium splnitelnosti* $\forall^2 \exists^*$-sentencí; ve druhém kroku dokážeme, že toto kritérium je *dostačující pro konečnou splnitelnost*. V Gödelově publikaci je druhá část náročnou a velmi sofistikovanou modelovou konstrukcí. My namísto ní použijeme o hodně jednodušší pravděpodobnostní argument podle Gureviche a Shelaho.

Fakticky si dokážeme obecnější výsledek, který se týká sentencí $\forall^2\exists^*$, které mohou obsahovat rovnost. Musíme však splnit jistou sémantickou podmínku: každá splnitelná sentence musí mít model, v němž žádný element není jedinečně určen svým atomickým typem. Jak ukážu níže, tato podmínka je splněna všemi sentencemi bez rovnosti, ale existují i další zajímavé případy. Například dojdu k závěru, že fragment $\forall^2\exists^*$ teorie grafů je rozhodnutelný. Rovněž rozhodnutelnost Ackermannovy třídy s rovností je důsledkem tohoto výsledku.

Gödelovo kritérium. Nechť $\psi = \forall x \forall y \exists z_1 \ldots\ldots \exists z_m \varphi(x, y, z_1, \ldots, z_m)$ je relační sentence prvního řádu (s případnou rovností), kde φ je bez kvantifikátorů. Na strukturách s alespoň dvěma elementy je ψ ekvivalentní

$$\forall x \forall y \exists z_1 \ldots\ldots \exists z_m \exists z'_1 \ldots\ldots \exists z'_m (x = y \supset \varphi(x, x, z_1, \ldots, z_m) \wedge \varphi(x, y, z'_1, \ldots, z'_m)).$$

Dále platí, že na dostatečně velkých strukturách můžeme zavést nerovnosti proměnných opakovaným použitím ekvivalence

$$\exists x \exists y \alpha(x, y) \equiv \exists x \exists y((\alpha(x, x) \vee \alpha(x, y)) \wedge x = y),$$

můžeme tak omezit naši pozornost na sentence formy

$$\psi := \forall x_1 \forall x_2 \exists x_3 \ldots\ldots \exists x_m (x_1 = x_2 \supset \varphi(x_1, x_2, \ldots, x_m)),$$

kde $\varphi(x_1, \ldots, x_m) \models \bigwedge_{1 \leq i < j \leq m} x_i \neq x_j$, a na struktury s alespoň *m* elementy. Takovým sentencím říkáme *Gödelovy sentence speciální formy*.

Definice 4.2.1.2.2. *k-tabulka* slovní zásoby σ, je σ-strukturou s univerzem $\{1, \ldots, k\}$. Dále platí, že s ohledem na danou strukturu $\mathfrak{A}$ s *k*-násobnou $a_1, \ldots, a_k$ rozdílných prvků, je $T_{\mathfrak{A}}[a_1, \ldots, a_k]$ jedinečnou *k*-tabulkou, která je izomorfická, prostřednictvím mapování $i \rightarrow a_i$ (pro $i = 1, \ldots, k$) na substrukturu $\mathfrak{A}$ indukovanou $a_1, \ldots, a_k$.

Definice 4.2.1.2.3. Element *a* nějaké substruktury $\mathfrak{A}$ je *král*, pokud v $\mathfrak{A}$ neexistuje žádný další element *b* se stejnou 1-tabulkou, tzn. s $T_{\mathfrak{A}}[b] = T_{\mathfrak{A}}[a]$.

Lemma 4.2.1.2.4. *Nechť ψ je libovolná relační sentence prvního řádu bez rovnosti. Pokud ψ je splnitelná, pak má model bez králů.*

Důkaz. Předpokládejte, že $\mathfrak{A}$ je model pro ψ s univerzem *A*. Nechť $2\mathfrak{A}$ je struktura s univerzem $A \times \{0, 1\}$ a relacemi definovanými takovým způsobem, že

$$2\mathfrak{A} \models R((a_1, i_1) \ldots (a_k, i_k)) \Leftrightarrow \mathfrak{A} \models Ra_1 \ldots a_k$$

pro všechny *k*-ární predikáty *R* a všechny $a_1, \ldots, a_k \in A$ a $i_1, \ldots, i_k \in \{0, 1\}$. Je zřejmé, že $\mathfrak{A}$ a $2\mathfrak{A}$ jsou nerozlišitelné sentence bez rovnosti a že $2\mathfrak{A}$ neobsahuje krále.

Definice 4.2.1.2.5 (Gödelovo kritérium). Nechť $\varphi(x_1, \ldots, x_m)$ je bez kvantifikátorů a *P, Q* jsou neprázdné množiny 1-tabulek a 2-tabulek v tomto pořadí nad σ. Říkáme, že *P, Q* splňují Gödelovo kritérium pro φ, pokud

(1) pro všechna $\mathfrak{B}, \mathfrak{B}' \in P$, existuje nějaká 2-tabulka $\mathfrak{C} \in Q$, tak že platí $T_{\mathfrak{C}}[1] = \mathfrak{B}$ a $T_{\mathfrak{C}}[2] = \mathfrak{B}'$.

(2) každé 2-tabulky $\mathfrak{B} \in Q$ lze rozšířit na *m*-tabulku $\mathfrak{C}$ tak, že

- $T_{\mathfrak{C}}[1, 2] = \mathfrak{B}$;
- $T_{\mathfrak{C}}[i] \in P$ pro všechna $i \in \{1, \ldots, m\}$;
- $T_{\mathfrak{C}}[i, j] \in Q$ pro všechna rozdílná $i, j \in \{1, \ldots, m\}$;
- $\mathfrak{C} \models \varphi[1, \ldots, m]$.

Lemma 4.2.1.2.6. *Nechť* $\psi = \forall x_1 \forall x_2 \exists x_3 \ldots\ldots \exists x_m(x_1 \neq x_2 \supset \varphi(x_1, x_2, \ldots, x_m))$ *je Gödelova sentence ve speciální formě. Pokud má* ψ *model bez králů, pak existují neprázdné množiny P a Q, které splňují Gödelovo kritérium pro* φ.

Důkaz. Zvolte si model $\mathfrak{A} \models \psi$ bez králů a nastavte

$$P := \{T_{\mathfrak{A}}[a] : a \in A\}$$

$$Q := \{T_{\mathfrak{A}}[a, b] : a, b \in A, a \neq b\}.$$

Dostatečnost Gödelova kritéria pro konečnou splnitelnost.

Výrok 4.2.1.2.7. *Nechť* $\psi = \forall x_1 \forall x_2 \exists x_3 \ldots\ldots \exists x_m(x_1 \neq x_2 \supset \varphi(x_1, \ldots, x_m))$ *je nějaká Gödelova sentence ve speciální formě a předpokládejme, že P a Q splňují Gödelovo kritérium pro* φ. *Pak má* ψ *konečný model.*

Důkaz. Nechť $P = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_p\}$. Pro $n \geq m$ předkládáme pravděpodobnostní konstrukci jedné *np*-tabulky $\mathfrak{A}$:

Stupeň 1: Každý prvek univerza $\{1, \ldots, np\}$, lze zapsat ve formě $ip + j$, kde $0 \leq i < n$, $1 \leq j \leq p$. Nastavíme $T_{\mathfrak{A}}[ip + j] := \mathfrak{B}_j$.

Stupeň 2: Nechť $1 \leq a < b \leq np$. Podle podmínky (1) Gödelova kritéria je množina

$$\{\mathfrak{C} \in Q : T_{\mathfrak{C}}[1] = T_{\mathfrak{C}}[a],\ T_{\mathfrak{C}}[2] = T_{\mathfrak{A}}[b]\}$$

neprázdná. Vyberte náhodným způsobem 2-tabulku $\mathfrak{C}$ z této množiny a položte $T_{\mathfrak{A}}[a, b] := \mathfrak{C}$.

Stupeň j $(3 \leq j \leq m)$*:* Definujte pravdivostní hodnotu každého atomického výroku $Ra_1 \ldots. a_k$, pro kterou má $a_1 \ldots. a_k$ přesně *j* rozdílných komponent, a to náhodně s pravděpodobností $1/2$.

Stupeň m + 1, m + 2, . . . : Nastavte $\mathfrak{A} \models \neg Ra_1 \ldots a_k$ pro každý relační symbol a každou uspořádanou n-tici $a_1 \ldots a_k$ s více než *m* rozdílnými komponentami.

Všimněte si, že ve stupni *j* jsou určeny pravděpodobnostní hodnoty všech atomických výroků na *j* rozdílných elementech. Nechť S_n je množinou všech *np*-tabulek, u kterých se může jevit, že mají pozitivní pravděpodobnost jako výsledek tohoto pravděpodobnostního procesu. S_n považujeme za pravděpodobnostní prostor s rovnoměrnou distribucí pravděpodobnosti.

Definice 4.2.1.2.8. Nechť $\mathfrak{A} \in S_n$, $a_1, \ldots, a_m \in \{1, \ldots, np\}$ a nechť $\mathfrak{C}$ je *m*-tabulka. Říkáme, že $a_3, \ldots, a_m$, *jsou svědky* $\mathfrak{C}$ *pro* a_1, a_2, pokud

$\mathfrak{A} \models Ra_{i1} \ldots\ldots a_{ik} \Leftrightarrow \mathfrak{C} \models Ri_1 \ldots\ldots i_k$,

pro všechny *k*-nární relační symboly $R \in \sigma$ a všechny $i_1, \ldots, i_k \in \{1, \ldots, m\}$takové, že platí $i_j > 2$ pro alespoň jedno *j*. Všimněte si, že pro případ, kdy σ obsahuje pouze unární a binární predikáty, má toto za následek, že platí

$T_{\mathfrak{A}}[a_1, a_j] = T_{\mathfrak{C}}[i, j]$

pro všechna $i \neq j$ s $i > 2$ nebo $j > 2$.

Nechť *s* je počet atomů $Rx_{i1} \ldots\ldots x_{ik}$ tak, že platí: *R* je *k*-nární predikát v σ s $3 \leq k \leq m$ a zároveň platí, že $i_1, \ldots, i_k$ je uspořádaná n-tice čísel v množině $\{1, \ldots, m\}$ s alespoň třemi různými komponentami. Dále nechť platí, že

$$r := \binom{m-2}{2} + 2(m-2)$$

$$q := |Q|$$

$$\varepsilon := \frac{1}{q^r * 2^r}$$

Podle podmínky (2) Gödelova kritéria existuje funkce *f*, která přiřazuje každé 2-tabulce $\mathfrak{B} \in Q$ nějakou vhodnou *m*-tabulku $f(\mathfrak{B})$. Podmíněnou pravděpodobnost, že nastane událost *E* za předpokladu, že nastala událost *F*, zapisujeme pro libovolné události *E a F* obvykle ve tvaru Pr[*E* | *F*].

Lemma 4.2.1.2.9. *Nechť* $\mathfrak{B} \in Q$, $\mathfrak{C} = f(\mathfrak{B})$ *a nechť* $a_1, \ldots, a_m$ *je m rozdílných prvků z* $\{1, \ldots, np\}$. *Pak je podmíněná pravděpodobnost*

Pr[$a_3, \ldots, a_m$ *jsou svědky* $\mathfrak{C}$ *pro* $a_1, a_2 \mid T_{\mathfrak{A}}[a_i] = T_{\mathfrak{C}}[i]$ *pro* $i = 1, \ldots, m$]

nejméně ε.

Důkaz. Existuje *s* atomů $Rx_{i1} \ldots\ldots x_{ik}$ s nejméně třemi rozdílnými proměnnými. Pro každou z nich platí, že

Pr[$\mathfrak{A} \models Ra_{i1} \ldots\ldots\ldots a_{ik}$] = 1 / 2.

Pravděpodobnost, že $\mathfrak{A} \models Ra_{i1} \ldots\ldots a_{ik}$, právě tehdy, když $\mathfrak{C} \models Ri_1 \ldots\ldots i_k$, pro všechny takové atomy, je tudíž 2^{-s}.

Odpovídající ekvivalence pro všechny atomy se dvěma rozdílnými proměnnými je taktéž platná, pokud

$T_{\mathfrak{A}}[a_i, a_j] = T_{\mathfrak{C}}[i, j]$,

pro všechna $i \neq j, \{i, j\} \neq \{1, 2\}$. Existuje r takových množin $\{i, j\}$. Odpovídajícím způsobem je poté – v případě, že toto platí pro všechna i, j - pravděpodobnost $\geq q^{-r}$. Pro atomy s pouze jednou proměnnou zůstává ekvivalence platná podle předpokladu.

Nechť $\ell := [(n-2)/(m-2)]$; v důsledku toho $n \geq \ell(m-2) + 2$.

Lemma 4.2.1.2.10. *Nechť a_1, a_2 jsou rozdílné elementy z $\{1, \ldots, np\}$. Potom platí*

$\Pr[\mathfrak{A} \models \neg\exists x_3 \ldots\ldots \exists x_m \varphi[a_1, a_2]] \leq (1-\varepsilon)^{\ell}$.

Důkaz. Nechť $\mathfrak{B}$ je jakákoliv možná hodnota pro $T_{\mathfrak{A}}[a_1, a_2]$ a $\mathfrak{C} = f(\mathfrak{B})$. Nyní je dostačující dokázat, že

$\Pr[$žádná uspořádaná n-tice $a_3, \ldots, a_m$ není svědkem $\mathfrak{C}$ pro $a_1, a_2] \leq (1-\varepsilon)^{\ell}$.

Podle této konstrukce, $\mathfrak{A}$ obsahuje alespoň $n-2 \geq \ell(m-2)$ párových rozdílných prvků $a_{i,j} \in \{1, \ldots, np\} - \{a_1, a_2\}$, tak že $T_{\mathfrak{A}}[a_{i,j}] = T_{\mathfrak{C}}[j]$ pro $i = 1, \ldots, l$ a $j = 3, \ldots, m$. ℓ událostí

"$a_{i,3}, \ldots, a_{i,m}$ jsou svědky $\mathfrak{C}$ pro a_1, a_2"

je nezávislých a mají pravděpodobnost $\geq \varepsilon$. Událost, že žádná n-tice $a_3, \ldots, a_m$ není svědkem $\mathfrak{C}$ pro a_1, a_2, má tak pravděpodobnost nejvýše $(1-\varepsilon)^{\ell}$.

Z toho vyplývá, že na S_n platí

$$\Pr[\mathfrak{A} \models \neg\psi] \leq \sum_{a_1 \neq a_2} \Pr[\mathfrak{A} \models \neg\exists x_3 \ldots \exists x_m \varphi[a_1, a_2]]$$

$$\leq pn(pn-1)(1-\varepsilon)^{\ell} \leq pn(pn-1)(1-\varepsilon)^{(n-2)/(m-2)-1},$$

což se exponenciálně přibližuje k 0 s tím, jak n narůstá. Pro dostatečně velké n je tak pravděpodobnost, že náhodně zvolené $\mathfrak{A} \in S_n$ je modelem pro ψ pozitivní. ψ je tudíž konečným modelem.

Jako důsledek získáváme

***Teorém* 4.2.1.2.11.** *Nechť ψ je jakákoliv relační sentence $\forall^2\exists^*$, která má model bez králů. Potom ψ je konečný model.*

Důkaz. Nechť $\mathfrak{A}$ je modelem pro ψ bez králů. Pokud je $\mathfrak{A}$ konečné, není potřeba nic dokazovat. V opačném případě transformujeme ψ na Gödelovu sentenci ve speciálním tvaru, která je ekvivalentní ψ na všech strukturách, jejichž kardinalita přesahuje počet proměnných v ψ. Na základě lemmy 4.2.1.2.6 existují P a Q, které splňují Gödelovo kritérium, což podle věty 4.2.1.2.7. má za následek to, že ψ má konečný model.

Jelikož každá splnitelná formule bez rovnosti má model bez králů, je důsledkem tohoto faktu vlastnost konečného modelu u [$\forall^2\exists^*$, all]. Výrok 4.2.1.2.1 (Gödel, Schütte) je tedy dokázán.

Teorii orientovaných grafů, lze považovat za teorii jedné nereflexivní binární relace. Jelikož jsou u nereflexivní relace všechny 1-tabulky identické, jsou tedy orientované grafy strukturami bez králů.

Důsledek 4.2.1.2.12. Fragment $\forall^2\exists^*$ teorie orientovaných grafů je rozhodnutelný.

Poznámka. Pomocí metody existenčních interpretací Gurevich ukázal, že fragment $\forall^3\exists^*$ této teorie je nerozhodnutelný.

Kompletní Gödel-Kalmár-Schütteova třída. Zde prezentujeme dvě metody rozšíření věty výroku 4.2.1.2.1 na [$\exists^*\forall^2\exists^*$, *all*].

První postup generalizuje Gödelovo kritérium pro sentence s existenčními kvantifikátory na začátku. Tentýž argument - jako výše uvedený - ukazuje, že můžeme soustředit naši pozornost na případ, kdy všechny proměnné je třeba interpretovat pomocí zvláštních elementů, tzn. do sentencí ve formě

$$\psi := \exists x_1 \cdot \cdot \cdot \exists x_p \forall y_1 \forall y_2 \exists z_1 \cdot \cdot \cdot \exists z_t(\alpha(\bar{x}, y_1, y_2) \supset \varphi(\bar{x}, y_1, y_2, \bar{z}),$$

kde $\alpha(\bar{x}, y_1, y_2)$ vyhrazuje rozlišnost mezi y_1, y_2 a $x_1, \ldots, x_p$, přičemž φ má za následek všechny zbývající nerovnosti mezi rozdílnými proměnnými.

Definice 4.2.1.2.13. (Rozšířené Gödelovo kritérium). Nechť $\mathfrak{A}$ je p-tabulkou nad σ a P, Q nechť jsou neprázdné množiny (p+1)-tabulek a (p+2)-tabulek v tomto pořadí nad σ. Říkáme, že $\mathfrak{A}$, P, Q splňují rozšířené Gödelovo kritérium pro ψ, pokud

(0) pro každé $\mathfrak{B} \in P \cup Q$ platí, že $T_{\mathfrak{B}}[1, \ldots, p] = \mathfrak{A}$.

(1) pro každé $\mathfrak{B}, \mathfrak{B}' \in P$ existuje $(p + 2)$-tabulka $\mathfrak{C} \in Q$ taková, že
$T_{\mathfrak{C}}[1, \ldots, p, p + 1] = \mathfrak{B}$ a $T_{\mathfrak{C}}[1, \ldots, p, p + 2] = \mathfrak{B}'$.

(2) Každou $(p + 2)$-tabulku $\mathfrak{B} \in Q$ lze rozšířit na m-tabulku $\mathfrak{C}$ tak, že platí

- $T_{\mathfrak{C}}[1, \ldots, p + 2] = \mathfrak{B}$;
- $T_{\mathfrak{C}}[1, \ldots, p, i] \in P$ pro všechna $i \in \{p + 1, \ldots, m\}$;
- $T_{\mathfrak{C}}[1, \ldots, p, i, j] \in Q$ pro všechna různá $i, j \in \{p + 1, \ldots, m\}$;

- $\mathfrak{C} \models \varphi[1, \ldots, m]$.

Důsledek 4.2.1.2.14. [$\exists^*\forall^2\exists^*$, *all*] *má vlastnost konečného modelu.*

Stejný výsledek je možno získat eliminací úvodních existenčních kvantifikátorů, čímž dojde k redukci prefixové třídy [$\exists^*\forall^2\exists^*$] na třídu [$\forall^2\exists^*$].

Příklady

Opět uvádím příklad, kdy daná formule splňuje podmínky této třídy a tudíž je i rozhodnutelná. Následují příklady, kdy formule tyto podmínky nesplňuje.

Příklad:

$\exists x(\exists y\exists z(\neg P(x, y) \wedge Q(z)) \supset \exists v P(x, v))$ – Výchozí formule

Nejdříve formuli převedeme na prenexní tvar a ověříme si, že splňuje podmínky Gödel-Kalmár-Schütteovské třídy.

Prenexní tvar
$\exists x(\exists y\exists z(\neg P(x, y) \wedge Q(z)) \supset \exists v\neg P(x, v)) \Rightarrow$ (*eliminace implikace*)

$\exists x(\forall y\forall z(P(x, y) \vee \neg Q(z)) \vee \exists v\neg P(x, v)) \Rightarrow$ (*přesun kvantifikátorů doleva*)

$\exists x\forall y\forall z\exists v(P(x, y) \vee \neg Q(z) \vee \neg P(x, v))$ – *prenexní tvar formule.*

Formule v prenexním tvaru splňuje podmínky této třídy. Pojďme si tedy ukázat důkaz této formule. Formuli nejprve znegujeme a poté postupně uplatňujeme skolemizaci.

Skolemizace
$\exists x(\exists y\exists z(\neg P(x, y) \wedge Q(z)) \supset \exists v\neg P(x, v)) \Leftrightarrow$ (*negace formule*)

$\forall x\neg(\exists y\exists z(\neg P(x, y) \wedge Q(z)) \supset \exists v\neg P(x, v)) \Leftrightarrow$ (*eliminace implikace*)

$\forall x\neg(\forall y\forall z(P(x, y) \vee \neg Q(z)) \vee \exists v\neg P(x, v)) \Leftrightarrow$ (*přesun negace dovnitř*)

$\forall x(\exists y\exists z(\neg P(x, y) \wedge Q(z)) \wedge \forall v P(x, v)) \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\forall x(\neg P(x, f(x)) \wedge Q(g(x)) \wedge \forall v P(x, v)) \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x\forall v(\neg P(x, f(x)) \wedge Q(g(x)) \wedge P(x, v))$

Rezoluce
1. $\neg P(x, f(x))$
2. $Q(g(x))$
3. $P(x, v)$
4. #spor rezoluce 1, 2 v/f(x)

Došli jsme ke sporu, tudíž je původní formule logicky pravdivá.

Následuje několik příkladů formulí, které nesplňují podmínky této podtřídy, tudíž nejsou rozhodnutelné.

Protipříklad

$\exists x \forall y[(\neg P(x,y) \supset Q(f(a), z)) \supset \exists z_1(P(z_1,y) \vee Q(x,x))]$ – výchozí formule

Vidíme, že formule obsahuje funkční symbol *f(a)*, kterého bychom se ani převodem na prenexní tvar nezbavili. Tím pádem už nyní formule nesplňuje podmínky této třídy. Nicméně provedeme důkaz této formule.

Formuli znegujeme a přejmenujeme proměnné a uplatňujeme algoritmus skolemizace.

Skolemizace
$\exists x \forall y[(\neg P(x,y) \supset Q(f(a), z)) \supset \exists z_1(P(z_1,y) \vee Q(x,x))] \Leftrightarrow$ (*negace a přejmenování proměnných*)

$\exists z \forall x \exists y[(\neg P(x,y) \supset Q(f(a), z)) \wedge \forall z_1(\neg P(z_1,y) \wedge \neg Q(x,x))] \Leftrightarrow$ (*eliminace implikace*)

$\exists z \forall x \exists y[(P(x,y) \vee Q(f(a), z)) \wedge \forall z_1(\neg P(z_1,y) \wedge \neg Q(x,x))] \Rightarrow$ (*eliminace existenčních kvant.*)

$\forall x [(P(x, g(x)) \vee Q(f(a), b)) \wedge \forall z_1(\neg P(z_1, g(x)) \wedge \neg Q(x,x))] \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall z_1[(P(x, g(x)) \vee Q(f(a), b)) \wedge (\neg P(z_1, g(x)) \wedge \neg Q(x,x))]$

Vypíšeme klausule pod sebe a budeme provádět unifikaci literálů, tj. substituci termů za proměnné tak, abychom mohli uplatnit rezoluční pravidlo.

Rezoluce
1. $P(x, g(x)) \vee Q(f(a), b))$
2. $\neg P(z_1, g(x))$
3. $\neg Q(x,x))$
4. $Q(f(a), b)$ rezoluce 1, 2 x/z_1

Nelze dále unifikovat; nedošli jsme ke sporu, tím pádem původní formule není tautologie.

Protipříklad 2

$[\forall x(P(x) \supset \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \supset \exists x Q(x,a)$ – Výchozí formule.

U této formule nejde takto předem říct, jestli splňuje podmínky této rozhodnutelné třídy. Proto ji nejprve převedeme na prenexní tvar a poté můžeme rozhodnout.

Převod na prenexní tvar
$[\forall x(P(x) \supset \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \supset \exists x Q(x,a) \Leftrightarrow$ (*eliminace implikace*)

$\neg[\forall x(\neg P(x) \vee \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \vee \exists x Q(x,a) \Leftrightarrow$ (*přesun negace dovnitř*)

$[\exists x(P(x) \wedge \forall y \exists z(\neg P(y) \vee \neg Q(y, z) \vee \neg Q(x, z)))] \vee \exists x Q(x,a) \Leftrightarrow$ (*přejmenovaní proměnných*)

$[\exists x(P(x) \wedge \forall y \exists z(\neg P(y) \vee \neg Q(y, z) \vee \neg Q(x, z)))] \vee \exists x_1 Q(x_1,a) \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\exists x \forall y \exists z \exists x_1[(P(x) \wedge (\neg P(y) \vee \neg Q(y, z) \vee \neg Q(x, z)))] \vee Q(x_1,a)]$

Formule v prenexním tvaru neobsahuje požadovaný prefix. Nesplňuje tak omezení Gödel-Kalmár-Schütteovské třídy. Nyní si ještě dokážeme její důkaz.

Původní formuli opět znegujeme, přejmenujeme proměnné a budeme postupně uplatňovat algoritmus skolemizace.

Skolemizace

$[\forall x(P(x) \supset \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \supset \exists x Q(x,a) \Leftrightarrow$ (*negace formule*)

$\neg[[\forall x(P(x) \supset \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \supset \exists x Q(x,a)] \Leftrightarrow$ (*eliminace implikace*)

$\neg[[\neg \forall x(\neg P(x) \vee \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \vee \forall x Q(x,a)] \Leftrightarrow$ (*přejmenování proměnných*)

$\neg[[\neg \forall x(\neg P(x) \vee \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \vee \forall x_1 Q(x_1,a)] \Leftrightarrow$ (*přesun negace dovnitř*)

$[\forall x(\neg P(x) \vee \exists y \forall z(P(y) \wedge Q(y, z) \wedge Q(x, z)))] \vee \forall x_1 Q(x_1,a) \Rightarrow$ (*eliminace existenčních kvant.*)

$[\forall x(\neg P(x) \vee \forall z(P(b) \wedge Q(b, z) \wedge Q(x, z)))] \vee \forall x_1 Q(x_1,a) \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall z \forall x_1[(\neg P(x) \vee (P(b) \wedge Q(b, z) \wedge Q(x, z))) \vee Q(x_1,a))] \Leftrightarrow$ (*distributivní zákony*)

$\forall x \forall z \forall x_1\{[(\neg P(x) \vee (P(b)) \wedge (\neg P(x) \vee Q(b, z)) \wedge (\neg P(x) \vee Q(x, z))] \vee Q(x_1,a)\} \Leftrightarrow$ (*distributivní zákony*)

$\forall x \forall z \forall x_1\{[(\neg P(x) \vee (P(b) \vee Q(x_1,a)) \wedge (\neg P(x) \vee Q(b, z) \vee Q(x_1,a)) \wedge (\neg P(x) \vee Q(x, z) \vee Q(x_1,a))]\}$

Rezoluce

1. $\neg P(x) \vee P(b) \vee Q(x_1,a)$
2. $\neg P(x) \vee Q(b, z) \vee Q(x_1,a)$
3. $\neg P(x) \vee Q(x, z) \vee Q(x_1,a)$
4. $\neg P(b)\ Q(b, z) \vee Q(x_1,a)$ rezoluce 1, 2 x/b

Nedošli jsme ke sporu - negovaná formule je splnitelná, původní tedy není tautologie.

4.2.1.3 Bernays-Schönfinkelova třída

Bernays-Schönfinkelova třída (známá také jako Bernays–Schönfinkel-Ramseyova třída = BSR) je třída všech formulí, v jejichž prenexní normální formě vystupují nejprve kvantifikátory existenční a pak teprve všechny všeobecné (∃*∀*) viz také:

$\exists x_1 \cdot \cdot \cdot \exists x_n \forall x_1 \forall y_2 \cdot \cdot \cdot \forall y_m \varphi,$

kde φ neobsahuje žádné další kvantifikátory a žádné funkční symboly. Bernays a Schönfinkel dokázali, že problém splnitelnosti - pro sentence bez rovnosti a s prefixem ∃*∀* - je rozhodnutelný. Ramsey rozšířil tyto výsledky na výroky ∃*∀* s rovností a ukázal, že spektrum každé takové sentence je buďto konečné nebo kokonečné. V této sekci dokazujeme, že problém logické pravdivosti pro sentence ∃*∀* bez funkcí je kompletní pro non-deterministický exponenciální čas, a to bez ohledu na to, zda formule obsahují rovnost nebo ne.

Rozhodnutelnost této třídy

Prvně ukazujeme, že každá relační sentence $\psi := \exists x_1 \ldots \exists x_p \forall y_1 \ldots \forall y_m \varphi$ je buďto neřešitelná nebo má model kardinality nejvýše *p*. Existuje několik způsobů jak toto dokázat. My použijeme jednoduchý modelově-teoretický argument založený na uzavření univerzálních sentencí pod substrukturami.

Pokud je $\mathfrak{A}$ substrukturou $\mathfrak{B}$ a $\mathfrak{B}$ je model sentence η v prenexním tvaru - který obsahuje pouze všeobecné kvantifikátory - pak rovněž platí, že $\mathfrak{A} \models \eta$.

Příklad: *Nechť* $\psi := \exists x_1 \ldots \exists x_p \forall y_1 \ldots \forall y_m \varphi$ *je řešitelnou sentencí v* $[\exists^* \forall^*, all]_=$. *Potom* ψ *má model s nejvýše max(1, p) elementy.*

Důkaz. Nechť σ je jazykem ψ. Jelikož ψ je splnitelné, existuje σ-struktura $\mathfrak{A}$ a prvky $a_1, \ldots, a_p$ tak, že platí:

$\mathfrak{A} \models \forall y_1 \ldots \forall y_m \varphi[a_1, \ldots, a_p]$

$\eta := \forall y_1 \ldots \forall y_n \varphi$ považujeme za sentenci expandované slovní zásoby $\tau = \sigma \cup \{a_1, \ldots, a_p\}$ a $(\mathfrak{A}, a_1, \ldots a_p)$ za τ -expanzi $\mathfrak{A}$. Jelikož η je univerzální, splňuje jej každá substruktura $(\mathfrak{A}, a_1, \ldots, a_p)$, tzn. každá τ –struktura $(\mathfrak{B}, a_1, \ldots, a_p)$, kde $\mathfrak{B} \subseteq \mathfrak{A}$ je substruktura $\mathfrak{A}$ obsahující $a_1, \ldots, a_p$.

Toto konkrétně platí pro univerzum $\{a_1, \ldots, a_p\}$ (pro případ, kdy $p = 0$, bereme jakoukoliv substrukturu kardinality jedna).

Příklady

Opět uvádím příklad, kdy daná formule splňuje podmínky této třídy. Následují příklady, kdy formule tyto podmínky nesplňuje.

Příklad:

$\forall x(A(x) \supset B(x)) \equiv \exists xQ(x)$ - Výchozí formule

Převod formule na prenexní normální tvar:
$(\forall x(A(x) \supset B(x)) \supset \exists xQ(x)) \wedge (\exists xQ(x) \supset \forall x(A(x) \supset B(x))) \Leftrightarrow$ (*eliminace ekvivalence*)

$(\neg\forall x(\neg A(x) \vee B(x)) \vee \exists xQ(x)) \wedge (\neg\exists xQ(x) \vee \forall x(\neg A(x) \vee B(x))) \Leftrightarrow$ (*eliminace implikace*)

$(\exists x \neg(\neg A(x) \vee B(x)) \vee \exists xQ(x)) \wedge (\forall x \neg Q(x) \vee \forall x(\neg A(x) \vee B(x))) \Leftrightarrow$ (*přesun negace dovnitř*)

$(\exists x(A(x) \wedge \neg B(x)) \vee \exists xQ(x)) \wedge (\forall x \neg Q(x) \vee \forall x(\neg A(x) \vee B(x))) \Leftrightarrow$ (*přejmenovaní proměn.*)

$(\exists w(A(w) \wedge \neg B(w)) \vee \exists xQ(x)) \wedge (\forall y \neg Q(y) \vee \forall z(\neg A(z) \vee B(z))) \Leftrightarrow$ (*přesun kvant. doleva*)

$\exists w\exists x((A(w) \wedge \neg B(w)) \vee Q(x)) \wedge \forall y\forall z\ (\neg Q(y) \vee (\neg A(z) \vee B(z))) \Leftrightarrow$ (*přesun kvant. doleva*)

$\exists w\exists x\forall y\forall z((A(w) \wedge \neg B(w)) \vee Q(x)) \wedge (\neg Q(y) \vee \neg A(z) \vee B(z))) \Leftrightarrow$ (*distributivní zákony*)

$\exists w\exists x\forall y\forall z[(A(w) \vee Q(x)) \wedge (\neg B(w) \vee Q(x)) \wedge (\neg Q(y) \vee \neg A(z) \vee B(z))]$

Formule v prenexním tvaru má prefix $\exists^*\forall^*$ a neobsahuje žádné další kvantifikátory a funkční symboly, proto splňuje omezení této třídy.

Příklad 2:

$\exists x\exists y\exists w\forall z(P(x,y) \supset Q(w,z))$

Převod na prenexní tvar
$\exists x\exists y\exists w\forall z(\neg P(x,y) \vee Q(w,z))$

Tato formule v prenexním tvaru splňuje podmínky Bernays- Schönfinkelovy třídy.

Pro ukázku si ještě ukážeme několik příkladů formulí, které nesplňují podmínky této podtřídy, tudíž nejsou rozhodnutelné.

Protipříklad:

$\exists z\exists x[[(\neg P(x) \supset Q(x,h(a)) \wedge \neg P(f(y))] \supset Q(x,y)]$ - Výchozí formule

U této formule už nyní můžeme říct, že nesplňuje omezení této podtřídy. Obsahuje totiž funkční symboly, kterých bychom se ani po převedení na prenexní tvar nezbavily. Proto rovnou přistoupíme k důkazu splnitelnosti formule.

Skolemizace
$\exists z\exists x[[(\neg P(x) \supset Q(x,h(a))) \wedge \neg P(f(y))] \supset Q(x,y)] \Leftrightarrow$ (*negace formule*)

$\forall z\forall x[[(\neg P(x) \supset Q(x,h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Rightarrow$ (*zavedení existenčního kvantifikátoru*)

$\exists y \forall z \forall x[[(\neg P(x) \supset Q(x,h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Leftrightarrow$ (*eliminace nadbytečných kvant.*)

$\exists y \forall x[[(\neg P(x) \supset Q(x,h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Leftrightarrow$ (*eliminace implikace*)

$\exists y \forall x[[(P(x) \vee Q(x,h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\forall x[[(P(x) \vee Q(x,h(a))) \wedge \neg P(f(b))] \wedge \neg Q(x,b)]$

Rezoluce:
1. $P(x) \vee Q(x,h(a))$
2. $\neg P(f(b))$
3. $\neg Q(x,b)$
4. $Q(f(b),h(a))$ rezoluce 1, 2 x/f(b)

Negovaná formule je splnitelná, původní tedy není tautologie.

Další protipříklady:

$\exists x \exists y \forall w \forall z(P(f(x),y) \supset Q(w,z))$

Tato formule má sice požadovaný prefix, ale obsahuje funkční symbol, tím pádem nesplňuje omezení dané třídy.

$\exists x \forall y \exists w \forall z(P(x,y) \supset Q(w,z))$ – tato formule nemá naopak požadovaný prefix.

V následující kapitole si rozebereme rozhodnutelné třídy formulí, které obsahují pouze jeden všeobecný kvantifikátor.

Formule s jedním ∀

V této sekci zkoumáme problém splnitelnosti u tříd formulí s jedním všeobecným kvantifikátorem. Prvně budeme uvažovat Gurevich-Maslov-Orevkovu třídu [∃*∀∃* , *all*, *all*], tzn. prefixovou třídu ∃*∀∃* v rámci predikátové logiky prvního řádu bez rovnosti, ale s libovolnými slovními zásobami, respektive počtem relačních a funkčních symbolů. Vlastnost konečného modelu u této třídy byla dokázána Gurevichem. Rozhodnutelnost jejího problému splnitelnosti (ne však vlastnost konečného modelu) byla rovněž dokázána Maslovem a Orevkovem.

Gurevich-Maslov-Orevkova třída je jedinečná maximální rozhodnutelná prefixová třída bez rovnosti, jelikož třída $\forall^2$ je konzervativní.

Rozhodnutelnost dokazujeme pomocí alternujícího testu splnitelnosti podle Grädela, který ukazuje, že tato třída se ve skutečnosti pro některá polynomiální *p* nachází v čase $\text{DTIME}(2^{p(n)})$. Rovněž zvážíme výsledky komplexity pro subtřídy [∃*∀∃*, *all*, *all*], jako jsou např. Ackermannova třída a monadická Ackermannova třída. Ukáže se, že většina z těchto tříd má deterministickou exponenciální časovou složitost. Nejlepší dolní meze složitosti pro tyto třídy je $\text{DTIME}(2^{(n/\log n)})$. Toto platí i pro třídu $[\forall\exists^2,(\omega)]$, která je fragmentem monadické Ackermannovy třídy. Pro tuto třídu bude ustanovena odpovídající horní meze složitosti.

U formulí s prefixem ∃*∀∃* s rovností je problém splnitelnosti rozhodnutelný pouze u relačních slovních zásob a pro slovní zásoby s nejvýše jedním funkčním symbolem. Relační formule ∃*∀∃* s rovností tvoří takzvanou Ackermannovu třídu s rovností. Pro tuto třídy dokazuji rozhodnutelnost a hranici složitosti v následující sekci. Druhá třída $[\exists^*\forall\exists^*, all, (1)]_=$ se nazývá Shelahova třída. Ze všech rozhodnutelných standardních tříd má nejvíce komplikovaný důkaz rozhodnutelnosti a budeme se jí zabývat v kapitole 4.2.2.2.

4.2.1.4 Gurevich-Maslov-Orevkovova třída

Gurevich-Maslov-Orevkovova třída, je třída všech těch formulí predikátové logiky prvního řádu bez rovnosti, jejichž prefix má v prenexní normální formě tvar ∃*∀∃*, viz také:

$\exists x_1 \cdot \cdot \cdot \exists x_n \forall x_1 \cdot \cdot \cdot \exists y_1 \cdot \cdot \cdot \exists y_n \varphi,$

formule φ není nijak omezená, co do počtu relačních a funkčních symbolů.

Test splnitelnosti pro [∃*∀∃*, *all*, *all*]

Výrok 4.2.1.4.1 (Grädel). *Problém splnitelnosti pro* [∃*∀∃*, *all, all*] je v DTIME($2^{p(n)}$), pro některý polynom *p*.

Prvně převedeme formule do Skolemovy normální formy a zredukujeme relační symboly na jeden unární predikát:

Lemma 4.2.1.4.2. *Existuje polynomiální redukce času, která převádí každou formuli* $\psi \in$ [∃*∀∃*, *all, all] na formuli* $\forall x\varphi$ *tak, že*

(i) φ *obsahuje konstanty, funkční symboly a jeden monadický predikát;*

(ii) délka φ *je lineární v délce* ψ*;*

(iii) ψ *je splnitelná tehdy a právě tehdy, když je splnitelná* $\forall x\varphi$.

Důkaz. Nejprve převedeme formuli $\psi := \exists y_1 \cdot \cdot \cdot \exists y_r \forall x \exists z_1 \cdot \cdot \cdot \exists z_t \alpha$ do Skolemovy normální formy $\forall x\beta$, kde β je získáno z α nahrazením každého y_i konstantou c_i a každého z_i za $F_i x$ (kde $F_1, \ldots, F_t$ jsou unární funkce, které se nevyskytují v α). Víme, že každá formule je splnitelná tehdy a právě tehdy, když je splnitelná její Skolemova forma.

Nyní zvolme nový monadický predikát Q a za každý predikát P v β novou funkci F_P, která má stejnou aritu jako P. Nahraďte každý atom $Pt_1 \cdot \cdot \cdot t_r$ v β za $QF_P\, t_1 \cdot \cdot \cdot t_r$. Nechť φ je výsledná formule.

Pokud $\forall x\varphi$ má model $\mathfrak{A}$, pak $\forall x\beta$ má model $\mathfrak{B}$ se stejným univerzem a stejnou interpretací konstant a funkčních symbolů. Interpretace relačního symbolu P je definována vztahem

$$\mathfrak{B} \models Pa_1 \cdot \cdot \cdot a_r \Leftrightarrow \mathfrak{A} \models QF_P(a_1, \ldots, a_r).$$

Nyní naopak předpokládejte, že $\mathfrak{B}$ je modelem pro $\forall x\beta$. Model se dvěma elementy je možné přímočaře zkonstruovat z modelu, který obsahuje pouze jeden element. Můžeme tudíž předpokládat, že $\mathfrak{B}$ má alespoň dva různé elementy a a b. Model $\mathfrak{A}$ pro $\forall x\varphi$ nad stejným univerzem (a se stejnou interpretací konstant) je definovaný následujícím způsobem:

$\mathfrak{A} \models Qa \wedge \neg Qb$

$$F_P^{\mathfrak{A}}(\mathrm{a}_1, \ldots, \mathrm{a}_r) := \begin{cases} a \ \ if \ \mathfrak{B} \models P\mathrm{a}_1 \ldots \mathrm{a}_r \\ b \ \ if \ \mathfrak{B} \models \neg P\mathrm{a}_1 \ldots \mathrm{a}_r \end{cases}$$

Jelikož se redukce skládá pouze z některých jednoduchých substitucí, je jasné, že ji lze spočítat v polynomiálním čase a že délka $\forall x\varphi$ je lineárně ohraničena v délce ψ.

Příklady

Následuje několik příkladů, kdy zadaná formule nesplňuje podmínky Gurevich-Maslov-Orevkovovy třídy.

Příklad

$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \supset \exists x Q(x)$ – Výchozí formule

Abychom zjistili, zda tato formule splňuje omezení Gurevich-Maslov-Orevkovovy třídy, převedeme ji na prenexní tvar.

Převod na prenexní tvar
$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \supset \exists x Q(x) \Rightarrow$ (*eliminace implikace*)

$[\exists x \forall y[\neg P(x,y)] \vee \exists x[P(a,x) \wedge \neg Q(x)]] \vee \exists x Q(x) \Rightarrow$ (*přejmenovaní proměnných*)

$[\exists x \forall y[\neg P(x,y)] \vee \exists x_1[P(a,x_1) \wedge \neg Q(x_1)]] \vee \exists x_2 Q(x_2) \Rightarrow$ (*přesun kvantifikátorů doleva*)

$\exists x \forall y \exists x_1 \exists x_2[\neg P(x,y) \vee (P(a,x_1) \wedge \neg Q(x_1)) \vee Q(x_2)]$

Formule v prenexním tvaru splňuje podmínky této podtřídy. Ukážeme si tedy ještě důkaz. Původní formuli znegujeme a převedeme na Skolemovu normální formu.

Skolemizace
$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \supset \exists x Q(x) \Leftrightarrow$ (*negace formule*)

$[\forall x \exists y[P(x,y)] \wedge \forall x[P(a,x) \supset Q(x)]] \wedge \forall x \neg Q(x) \Leftrightarrow$ (*přejmenování proměnných*)

$[\forall x \exists y[P(x,y)] \wedge \forall x_1[P(a,x_1) \supset Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Leftrightarrow$ (*eliminace implikace*)

$[\forall x \exists y[P(x,y)] \wedge \forall x_1[\neg P(a,x_1) \vee Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$[\forall x[P(x,f(x))] \wedge \forall x_1[\neg P(a,x_1) \vee Q(x_1)]] \wedge \forall x_2 \neg Q(x_2) \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall x_1 \forall x_2 [P(x,f(x)) \wedge (\neg P(a,x_1) \vee Q(x_1)) \wedge \neg Q(x_2)]$

Rezoluce

1. $P(x,f(x))$
2. $\neg P(a,x_1) \vee Q(x_1)$
3. $\neg Q(x_2)$
4. $\neg P(a,x_1)$ rezoluce 2, 3 x_2/x_1
5. #spor rezoluce 1, 4 $x_2/f(x)$ x/a

Došli jsme ke sporu, tudíž je původní formule logicky pravdivá.

Protipříklad

$\forall x[\neg P(x) \vee [\forall y[\neg P(y) \vee P(f(x))] \wedge \exists w[Q(x, w) \wedge \neg P(w)]]]$ – Výchozí formule

Nyní stačí přesunout kvantifikátory doleva, abychom dostali prenexní tvar formule.

$\forall x \forall y \exists w[\neg P(x) \vee [[\neg P(y) \vee P(f(x))] \wedge [Q(x,w) \wedge \neg P(w)]]]$ – prenexní tvar formule

Původní formuli znegujeme a budeme se snažit nalézt spor. Pokud je znegovaná formule kontradikce, pak je původní tautologie. Formuli znegujeme a přejmenujeme proměnné a uplatňujeme algoritmus skolemizace.

Skolemizace

$\forall x[\neg P(x) \vee [\forall y[\neg P(y) \vee P(f(x))] \wedge \exists w[Q(x, w) \wedge \neg P(w)]]] \Leftrightarrow$ (*negace formule*)

$\exists x[P(x) \wedge [\exists y[P(y) \wedge \neg P(f(x))] \vee \forall w[\neg Q(x, w) \vee P(w)]]] \Rightarrow$ (*eliminace existen. kvantifikátorů*)

$[P(a) \wedge [P(b) \wedge \neg P(f(a))] \vee \forall w[\neg Q(a, w) \vee P(w)]]] \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall w[P(a) \wedge P(b) \wedge \neg P(f(a)] \vee [\neg Q(a, w) \vee P(w)]] \Leftrightarrow$ (*distributivní zákony*)

$\forall w [(P(a) \vee \neg Q(a, w) \vee P(w)) \wedge (P(b) \vee \neg Q(a, w) \vee P(w)) \wedge (\neg P(f(a)) \vee \neg Q(a, w) \vee P(w)))]$

Vypíšeme klausule pod sebe a budeme provádět unifikaci literálů, abychom mohli uplatnit rezoluční pravidlo.

Rezoluce

1. $P(a) \vee \neg Q(a, w) \vee P(w)$
2. $P(b) \vee \neg Q(a, w) \vee P(w)$
3. $P(f(a)) \vee \neg Q(a, w) \vee P(w)$

Nelze nijak unifikovat. Negovaná formule je tedy splnitelná, původní formule tak není tautologie.

Protipříklad 2:

$\forall x \exists y \forall z[P(x, y) \supset (Q(y, z) \vee Q(x, y))]$ – Výchozí formule

Prefix této formule není ve tvaru ∃*∀∃*, tudíž nesplňuje podmínky této třídy. Nicméně původní formuli znegujeme a provedeme skolemizaci.

Skolemizace
$\forall x \exists y \forall z[P(x, y) \supset (Q(y, z) \vee Q(x, y))] \Leftrightarrow$ (*negace formule*)

$\exists x \forall y \exists z \neg[P(x, y) \supset (Q(y, z) \vee Q(x, y))] \Leftrightarrow$ (*eliminace implikace*)

$\exists x \forall y \exists z \neg[\neg P(x, y) \vee Q(y, z) \vee Q(x, y)] \Leftrightarrow$ (*přesun negace dovnitř*)

$\exists x \forall y \exists z[P(x, y) \wedge \neg Q(y, z) \wedge \neg Q(x, y)] \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\forall y[P(a, y) \wedge \neg Q(y, f(y)) \wedge \neg Q(a, y)]$

Sepíšeme si jednotlivé klausule pod sebe a budeme provádět unifikaci literálů, abychom mohli uplatnit rezoluční pravidlo.

Rezoluce
1. P(a, y)
2. ¬Q(y, f(y))
3. ¬Q(a, y)
4.

Výše dané klausule nejde dále unifikovat. Nedošli jsme tedy ke sporu a původní formule není tautologie.

4.2.1.5 Gurevichova třída

Gurevichova třída je třída všech těch formulí predikátové logiky s rovností, které v prenexní normální formě mají prefix ve tvaru ∃*. Formule dále musí obsahovat buďto dva funkční symboly nebo funkční a relační symbol či funkci s aritou větší než jedna. Tato třída má prefixový tvar:

$\exists x_1 \cdot \cdot \cdot \exists x_k \varphi$

Popíšeme si tedy standardní třídy, jejichž slovní zásoba obsahuje – jak jsem již zmínil - alespoň dvě funkce, nebo funkci a relaci, nebo funkci s aritou větší než jedna.

Dokážeme si následující výsledek:

Výrok 4.2.1.5.1. *Nechť X je prefixová třída slovní zásoby, jejíž slovní zásoba obsahuje alespoň dvě funkce, nebo funkci a relaci, nebo funkci s aritou větší než jedna. Pak Sat(X) je NP-těžké. Dále platí, že Sat(X) je NP-úplný tehdy a právě tehdy, když X obsahuje pouze existenční formule. V opačném případě je Sat(X) minimálně Pspace-těžký.*

Všimněte si, že třídy $[\forall, (0), (2)]_=$ a $[\forall, (0), (0, 1)]_=$ jsou neřešitelné. Předešlý výrok lze tak okamžitě odvodit z následujících předpokladů:

Propozice 4.2.1.5.2. Problém splnitelnosti u existenčních formulí prvního řádu, tzn. *Sat*[∃*, *all, all*]$_=$, je NP-úplný.

Nyní si všimněte si, že třída [∃*, *all, all*]$_=$ je jedna z maximálních řešitelných tříd - tedy Gurevichova třída.

Důkaz. Při dané existenční formuli $\exists x_1 \cdot \cdot \cdot \exists x_k \, \psi$, nechť T je množinou termů, které se vyskytují v ψ (třeba i jako podtermy nějakého dalšího termu). Pro každý term $s = fs_1 \cdot \cdot \cdot \, s_r$, který se vyskytuje v ψ, toto znamená, že T neobsahuje pouze s, ale také $s_1, \ldots, s_r$ a všechny jejich podtermy. Konkrétně platí, že T obsahuje všechny proměnné z ψ.

Nechť platí, že $T = \{t_1, \ldots, t_m\}$.ψ poté transformujeme na formuli:

$$\exists t_1 \, \cdots \, \exists t_m (\psi' \wedge \bigwedge_{\substack{s = f s_1 \ldots s_r \\ s \in T}} s \, = \, f s_1 \, \cdots \, s_r),$$

kde ψ' je stejná formule jako ψ, až na to, že termy ψ jsou v ψ' považovány za proměnné. Všechny atomy v této nové formuli jsou ve tvaru $Pz_1 \cdot \cdot \cdot \, z_r$, $z_1 = z_2$ a $fz_1 \cdot \cdot \cdot \, z_r = z_s$, kde všechna z_i jsou proměnné. Splnitelné formule v této formě mají model velikosti nanejvýš $k + m$. Existuje tudíž přímočarý postup jak rozhodnout splnitelnost existenčních formulí v nedeterministickém polynomiálním čase.

Navíc je tento problém s jistotou přinejmenším stejně náročný jako splnitelnost výrokových formulí, a je tudíž NP-uplný.

Propozice 4.2.1.5.3. *Pokud X obsahuje kterékoliv z následujících tří tříd*

$[\exists, (1), (1)]$ $[\exists, (0), (2)]_=$ $[\exists, (0), (0, 1)]_=$,

pak Sat(X) je NP-težké.

Důkaz. Nějaká výroková formule $\psi(X_1, \ldots, X_n)$ se nachází v SAT tehdy a právě tehdy, když jsou následující formule splnitelné:

- $\exists x \, \psi[X_i / P f^{i-1} x] \, \psi$
- $(\exists x) \, \psi[X_i / (g f^{i-1} x = x)]$
- $(\exists x) \, \psi[X_i / (f t_i x = x)]$, kde t_i jsou termy definované jako: $t_0 = x$ a $t_{i+1} = f x t_i$.

Příklady

Opět následuje několik příkladů, kdy zadaná formule nesplňuje podmínky Gurevichovy třídy. Tudíž tato formule není logicky pravdivá.

Protipříklad

$\exists z \exists x[[(\neg P(x) \supset Q(x, h(a))) \wedge \neg P(f(y))] \supset Q(x,y)]$ – Výchozí formule

Na první pohled by se mohl zdát, že daná formule splňuje podmínky této třídy – prefix je správný a navíc obsahuje dva výskyty funkčních symbolů. Nicméně daná formule neobsahuje symbol rovnosti. Můžeme si ukázat důkaz.

Původní formuli znegujeme a budeme se snažit nalézt spor. Pokud je znegovaná formule kontradikce, pak je původní tautologie.

Skolemizace
$\exists z \exists x[[(\neg P(x) \supset Q(x, h(a))) \wedge \neg P(f(y))] \supset Q(x,y)] \Leftrightarrow$ (*negace formule*)

$\forall z \forall x[[(\neg P(x) \supset Q(x, h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Rightarrow$ (*zavedení ∃, eliminace ∀)*

$\exists y \forall x[[(\neg P(x) \supset Q(x, h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Leftrightarrow$ (*eliminace implikace*)

$\exists y \forall x[[(P(x) \vee Q(x, h(a))) \wedge \neg P(f(y))] \wedge \neg Q(x,y)] \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\forall x[[(P(x) \vee Q(x, h(a))) \wedge \neg P(f(b))] \wedge \neg Q(x,b)]$

Nyní si sepíšeme jednotlivé klausule a budeme aplikovat rezoluční pravidlo.

Rezoluce:
1. $P(x) \vee Q(x, h(a))$
2. $\neg P(f(b))$
3. $\neg Q(x,b)$
4. $Q(f(b), h(a))$ rezoluce 1,2 x / f(b)

Nedošli jsme ke sporu, tím pádem původní formule není tautologií.

Protipříklad 2

$\{[\forall x[P(x) \supset \forall y(H(y) \supset R(x, y))] \wedge \exists x[P(x) \wedge \exists y \neg(R(x, y))] \supset \exists x H(x)]\}$ – Výchozí fomule

Už nyní opět můžeme konstatovat, že daná formule nesplňuje podmínky Gurevichovy třídy - neobsahuje funkční ani relační symboly. Pro úplnost si, ale ukážeme důkaz této formule. Původní formuli tedy znegujeme a převedeme na Skolemův tvar.

Skolemizace
$\{[\forall x[P(x) \supset \forall y(H(y) \supset R(x, y))] \wedge \exists x[P(x) \wedge \exists y \neg(R(x, y))] \supset \exists x H(x)]\} \Leftrightarrow$ (*negace formule*)

$\{[\forall x[P(x) \supset \forall y(H(y) \supset R(x, y))] \wedge \exists x[P(x) \wedge \exists y\neg(R(x, y))] \wedge \forall x\neg H(x)]\} \Leftrightarrow$ (*přejmenování proměnných*)

$\{[\forall x[P(x) \supset \forall y(H(y) \supset R(x, y))] \wedge \exists x_1[P(x_1) \wedge \exists y_1\neg(R(x_1, y_1))] \wedge \forall x_2\neg H(x_2)]\} \Leftrightarrow$ (*eliminace implikace*)

$\{[\forall x[\neg P(x) \vee \forall y(\neg H(y) \vee R(x, y))] \wedge \exists x_1[P(x_1) \wedge \exists y_1\neg(R(x_1, y_1))] \wedge \forall x_2\neg H(x_2)]\} \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\{[\forall x[\neg P(x) \vee \forall y(\neg H(y) \vee R(x, y))] \wedge [P(a) \wedge \neg(R(a, b))] \wedge \forall x_2\neg H(x_2)]\} \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x\forall y\forall x_2[(\neg P(x) \vee \neg H(y) \vee R(x, y)) \wedge P(a) \wedge \neg R(a, b) \wedge \neg H(x_2)]$

Rezoluce

1. $\neg P(x) \vee \neg H(y) \vee R(x, y)$
2. $P(a)$
3. $\neg R(a, b)$
4. $\neg H(x_2)$
5. $\neg H(y) \vee R(a, y)$ rezoluce 1,2 x/a
6. $\neg H(b)$ rezoluce 3,5 y/b

Nedošli jsme ke sporu; formule je tak splnitelná a původní není tautologie.

4.2.2 Rozhodnutelné třídy obsahující axiomy nekonečna

Ne všechny rozhodnutelné třídy v logice prvního řádu s prefixovou slovní zásobou mají vlastnost konečného modelu. Fakticky mezi sedmi maximálními rozhodnutelnými třídami, obsahují následující dvě axiomy nekonečna:

- Rabinova třída $[all,(\omega), (1)]_{=}$, tzn. logika prvního řádu s rovností, jednou unární funkcí a monadickými predikáty.
- Shelahova třída, tzn. třída $[\exists^*\forall\exists^*, all, (1)]_{=}$ prenexních sentencí prvního řádu s nejvýše jedním všeobecným kvantifikátorem, nejvýše jedním unárním funkčním symbolem a s libovolnými relačními symboly, s rovností, ale bez funkčních symbolů, které mají aritu > 1.

Opravdu je možné formulovat axiomy nekonečna s velmi skromnými kvantifikátorovými prefixy, a to i v teorii prvního řádu jedné unární funkce. Jelikož vlastnost konečného modelu nezůstává zachována, potřebujeme pro ustanovení rozhodnutelnosti rozdílné metody než v předcházející kapitole. Je třeba podotknout, že pro třídy s axiomy nekonečna jsou splnitelnost a konečná splnitelnost dva rozdílné problémy. Lze připustit, že jeden může být rozhodnutelný a ten druhý ne. Ukazuje se ovšem, že u tříd - které tady studujeme - lze dokázat s užitím stejných argumentů, že splnitelnost i konečná splnitelnost jsou rozhodnutelné.

Tyto výsledky se spoléhají na Rabinův slavný výsledek, který říká, že monadická teorie nekonečného binárního stromu *S2S* je rozhodnutelná. Toto je pro matematické teorie jeden z nejdůležitějších výroků o rozhodnutelnosti a má četné aplikace v několika oblastech matematiky a teorie informatiky. Důkaz, který je převážně podle Gureviche a Harringtona, nahrazuje nejkomplikovanější části Rabinovy studie (a to zvlášť komplementační výrok pro stromové automaty založené na indukci na počitatelných ordinálách) jednoduššími argumenty založenými na určitosti jistých her.

V následující sekci ukazuji, že monadickou teorii jedné unární funkce lze podobně jako mnohé další monadické teorie interpretovat v *S2S* a dokázat tak, že je rozhodnutelná. To, že problém splnitelnosti a konečné splnitelnosti u standardní třídy $[all, (\omega), (1)]_{=}$ v logice prvního řádu, je rozhodnutelný, což je jednoduchým důsledkem tohoto výsledku.

Ukazuji, že i teorie prvního řádu jedné unární funkce není elementárně rekurzivní, tzn. že její časová složitost převyšuje jakýkoliv konstantní počet iterací exponenciální funkce.

V sekci 4.2.2.2 dokazuji rozhodnutelnost Shelahovy třídy $[\exists^*\forall\exists^*, all, (1)]_{=}$ tím, že ji redukuji na fragment $\exists^*\forall\exists^*$ monadické teorie jedné unární funkce. Jde pravděpodobně o nejtěžší důkaz rozhodnutelnosti v této diplomové práci.

4.2.2.1 Rabinova třída

Rabinova třída patří mezi třídy formulí predikátové logiky s rovností, která obsahuje jednu unární funkci a pouze monadické predikáty. Zároveň u této třídy neplatí žádné omezení, co se týče prefixu formule.

Tvrzení 4.2.2.1.1 (Rabin). $\mathrm{Thm}(\mathrm{K}_f^{\omega})$, *monadická teorie unární funkce na vyčíslitelném oboru je rozhodnutelná.*

Důkaz. Nechť $\chi(x, y, Z)$ je SωS-formule

$\alpha(X, Z) := \forall x \exists y (X x \supset X y \wedge \chi(x, y, Z)$.

Pro všechny neprázdné $A, C \subseteq \omega^*$ platí, že $T^{\omega} \models \alpha[A, C]$ tehdy a právě tehdy, když (A, f_C) je podalgebra (B_C, f_C).

Jelikož může být každá vyčíslitelná algebra vnořena do ω-součtu obalujících algeber, vyplývá z toho, že pro libovolnou vyčíslitelnou algebru $\mathfrak{A}$ existují $A, C \subseteq \omega^*$ takové, že $T^{\omega} \models \alpha[A, C]$ a $\mathfrak{A} \simeq (A, f_C)$.

Nyní, nechť ψ je sentence monadické logiky jedné unární funkce. Bez újmy na obecnosti můžeme předpokládat, že ψ je v redukovaném tvaru neboli, že se funkce f vyskytuje pouze v atomech tvaru $fx = y$, kde x, y jsou proměnné. Pro překlad ψ do SωS-formule $\varphi(X, Z)$ nahraďte všechny atomy $fx = y$ za $\chi(x, y, Z)$, zrelativizujte všechny samostatné kvantifikátory na X a všechny množinové kvantifikátory na podmnožiny X. Pak ψ je tvrzení z $\mathrm{Thm}(\mathrm{K}_f^{\omega})$ tehdy a právě tehdy, když

$T^{\omega} \models \forall X \forall Z (\alpha(X, Z) \supset \varphi(X, Z))$.

To dokazuje, že Thm(K_f^ω) je rozhodnutelná.

Důsledek 4.2.2.1.2. *Slabá monadická teorie unární funkce na vyčíslitelném oboru je rozhodnutelná.*

Důkaz. Konečnost je definovatelná v SωS. Můžeme proto pozměnit překlad z ψ na $\varphi(X, Z)$ tak, že zrelativizujeme všechny množinové kvantifikátory na konečné podmnožiny X. Takto je také slabá monadická teorie jedné unární funkce v SωS interpretována.

Všimněte si, že Löwenheim-Skolemova věta se zobecňuje na monadickou logiku druhého řádu; jestliže má monadická sentence model, pak má (nejvýše) spočetný model. V důsledku je slabá monadická teorie unární funkce rozhodnutelná.

Splnitelnost

Důsledek 4.2.2.1.3. Problémy splnitelnosti a konečné splnitelnosti jsou u standardní třídy [*all*, (ω), (1)]$_=$ rozhodnutelné.

Důkaz. Nechť ψ je sentence prvního řádu s monadickými predikáty $Z_1, \ldots, Z_m$ a jednou unární funkcí. Pokud je ψ splnitelná, pak podle Löwenheim-Skolemovy věty platí, že ψ má spočetný model. ψ je tak nesplnitelná tehdy a pouze tehdy, pokud $\forall Z_1 \cdots \forall Z_m \neg\psi$ je věta Thm(K_f^ω).

Dále platí, že ψ nemá konečný model tehdy a pouze tehdy, pokud

$$\exists Y \forall z Yz \supset \forall Z_1 \cdots \forall Z_m \neg\psi$$

je výrok slabé monadické teorie jedné unární funkce. (Daný předpoklad nám říká, že Y je celé univerzum.). Podle výroku 4.2.2.1.1 a důsledku 4.2.2.1.2 (uvedených výše) jsou tyto problémy rozhodnutelné.

Příklady

Nyní opět následuje několik příkladů, kdy zadaná formule nesplňuje dané omezení Rabinovy třídy.

Protipříklad

$\neg[\forall x \exists y(P(x, y) \supset Q(x)) \wedge \neg\exists x Q(x) \wedge \neg\forall x \exists y P(x, y)]$ – Výchozí formule

Tato formule neobsahuje pouze monadické predikáty ani symbol rovnosti, takže nesplňuje podmínky Rabinovy třídy. Ukážeme si důkaz – znegujeme formuli a provedeme skolemizaci.

Skolemizace

$\neg[\forall x \exists y(P(x, y) \supset Q(x)) \wedge \neg\exists x Q(x) \wedge \neg\forall x \exists y P(x, y)] \Leftrightarrow$ (*negace*)

$[\forall x \exists y(P(x, y) \supset Q(x)) \wedge \neg\exists x Q(x) \wedge \neg\forall x \exists y P(x, y)] \Leftrightarrow$ (*eliminace implikace*)

$[\forall x \exists y(\neg P(x, y) \vee Q(x)) \wedge \forall x \neg Q(x) \wedge \exists x \forall y \neg P(x, y)] \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$[\forall x\,(\neg P(x, f(y)) \vee Q(x)) \wedge \forall x_1 \neg Q(x_1) \wedge \forall y \neg P(a, y)] \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall x_1 \forall y\,[(\neg P(x, f(y)) \vee Q(x)) \wedge \neg Q(x_1) \wedge \neg P(a, y)]$

Rezoluce

1. $\neg P(x, f(y)) \vee Q(x)$
2. $\neg Q(x_1)$
3. $\neg P(a, y)$
4. $\neg P(x, f(y))$ rezoluce $1, 2$ x / x_1

Nedošli jsme ke sporu a původní formule tedy není tautologie.

Protipříklad 2

$\{[\forall x(F(x) \supset (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x(H(x) \wedge \neg \exists y N(x, y)) \supset D(x))] \supset \forall x(F(x) \supset \exists y N(x, y))\}$ – Výchozí formule

Jak je vidět tato formule určitě nesplňuje podmínky této podtřídy. Neobsahuje pouze monadické predikáty a navíc ani neobsahuje jeden unární funkční symbol. Formuli znegujeme a ukážeme si její důkaz.

Skolemizace

$\{[\forall x(F(x) \supset (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x(H(x) \wedge \neg \exists y N(x, y)) \supset D(x))] \supset \forall x(F(x) \supset \exists y N(x, y))\} \Leftrightarrow$ (*negace formule*)

$\{[\forall x(F(x) \supset (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x(H(x) \wedge \neg \exists y N(x, y)) \supset D(x))] \wedge \exists x(F(x) \wedge \forall y \neg N(x, y))\} \Leftrightarrow$ (*přejmenování proměnných*)

$\{[\forall x(F(x) \supset (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x_1(H(x_1) \wedge \neg \exists y N(x_1, y)) \supset D(x_1))] \wedge \exists x_2(F(x_2) \wedge \forall y_1 \neg N(x_2, y_1))\} \Leftrightarrow$ (*eliminace implikace*)

$\{[\forall x(\neg F(x) \vee (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x_1(\neg H(x_1) \vee \exists y N(x_1, y)) \vee D(x_1))] \wedge \exists x_2(F(x_2) \wedge \forall y_1 \neg N(x_2, y_1))\} \Rightarrow$ (*eliminace existenčních kvantifikátorů*)

$\{[\forall x(\neg F(x) \vee (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\forall x_1(\neg H(x_1) \vee N(x_1, f(x_1))) \vee D(x_1))] \wedge (F(a) \wedge \forall y_1 \neg N(a, y_1))\} \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall x_1 \forall y_1 \{[\neg F(x) \vee (\neg H(x) \wedge \neg C(x) \wedge \neg K(x))] \wedge [\neg H(x_1) \vee N(x_1, f(x_1)) \vee D(x_1)] \wedge F(a) \wedge \neg N(a, y_1)\} \Leftrightarrow$ (*distributivní zákony*)

$\forall x \forall x_1 \forall y_1 \{[(\neg F(x) \vee \neg H(x)) \wedge (\neg F(x) \vee \neg C(x)) \wedge (\neg F(x) \vee \neg K(x))] \wedge [\neg H(x_1) \vee N(x_1, f(x_1)) \vee D(x_1)] \wedge F(a) \wedge \neg N(a, y_1)\}$

Rezoluce

1. $\neg F(x) \vee \neg H(x)$
2. $\neg F(x) \vee \neg C(x)$

3. $\neg F(x) \vee \neg K(x)$

4. $\neg H(x_1) \vee N(x_1, f(x_1)) \vee D(x_1)$

5. $F(a)$

6. $\neg N(a, y_1)$

7. $\neg H(a) \vee D(a)$ rezoluce 4,6 $y_1/f(x_1)$ x_1/a

8. $\neg C(a)$ rezoluce 2,5 x/a

9. $\neg H(a)$ rezoluce 1,5 x/a

Opět jsme nedošli ke sporu.

4.2.2.2 Shelahova třída

Shelahova třída je standardní fragment predikátové logiky prvního řádu s rovností. Jedná se sentenci, kdy formule φ je ve tvaru prenexní normální formy a splňuje následující podmínky:

- Prefix formule je ve tvaru $\exists^*\forall\exists^*$.
- Formule neobsahuje žádné funkční symboly s aritou vetší nebo rovno 2. Formule dále obsahuje nejvýše jeden unární funkční symbol. Neplatí zde žádné omezení na počet predikátů či jejich arit.

Problém logické pravdivosti je pomocí Shelahovy třídy rozhodnutelný.

Splnitelnost

Problém splnitelnosti u Shelahových sentencí je redukován na problém splnitelnosti u sentencí kanonických. Než tedy přistoupíme k samotnému důkazu, objasníme si pojem kanonických sentencí.

Kanonické sentence

Sentence jako sady klausulí. Jak je obvyklé, *hloubka* termu je definována indukcí: Hloubka individuální konstanty nebo proměnné je nula a zároveň platí: Hloubka(Par(t)) = 1+ Hloubka(t). *Literál* je atomická formule nebo její negace.

Pokud α je atomická formule, pak $+\alpha$ je α a $-\alpha$ je negací α. *Konstituční termy* atomické formule $P(t_1, \ldots, t_r)$ jsou termy $t_1, \ldots, t_r$, a *konstituční termy* neatomické formule φ jsou konstitučními termy atomických subformulí formule φ. Predikát (což je relační jméno) je *řádný*, pokud se liší od rovnítka. Literál $\pm P(t_1, \ldots, t_r)$ je *řádný* pokud je řádný i predikát P.

Definice 4.2.2.2.1. Literál α je *přípustný*, pokud má jednu z tří následujících forem:

- řádný literál se všemi konstitučními termy s hloubkou 0,
- nerovnosti s oběma konstitučními termy hloubky 0,

- rovnost t_1 = Par(t_2), kde každé t_i je hloubky 0.

Proměnou *u,* si vyhrazujeme pro použití s všeobecným kvantifikátorem — jde o *univerzální proměnnou*. Všechny ostatní proměnné jsou *existenční*. (V této sekci nebudeme uvažovat formule s více než jedním všeobecným kvantifikátorem.)

Řetězce jakékoliv uspořádané abecedy jsou uspořádané lexikograficky (pokud s_1 je řádný prefix s_2, pak s_1 v lexikografickém pořadí předchází s_2). Lexikografické pořadí je absolutní. Bez ztráty obecnosti předpokládáme, že konstanty a proměnné jsou řetězce v některé konečné abecedě a že všechny konstanty jsou lexikograficky před proměnnými a zároveň univerzální proměnná *u* je lexikograficky první proměnnou.

Definice 4.2.2.2.2. *Klausule K,* je konjunkcí přípustných literálů (nazývané *konstituční literály K*), které splňují následující podmínky:

- Pokud se netotožné proměnné v_1, v_2 vyskytují v *K* a v_1 lexikograficky předchází v_2, pak *K* obsahuje nerovnost $v_1 \neq v_2$.

- Pokud se některá existenční proměnná *v* a konstanta *c* nachází v *K,* pak *K* obsahuje literál $c \neq v$.

- Pokud se v *K* nachází některá konstanta *c*, pak *K* obsahuje buďto rovnost $c = u$ nebo nerovnost $c \neq u$.

Pokud se v klausuli *K* nachází některá proměnná *v* a konstanta *d* se v ní nenachází, pak $K(v / d)$ je klausule získaná z *K* nahrazení *v* za *d* a provedením očividných přídavných změn pro zajištění toho, aby byl výsledek klausule. Nechť EV(*K*) je kolekcí existenčních proměnných nějaké klausule *K*.

Definice 4.2.2.2.3. *E-uzavřené* klausule *K* s existenčními proměnnými $v_1, \ldots, v_m$ je formule $(\exists v_1 \ldots \exists v_m) K$.

Definice 4.2.2.2.4. Sentence prvního řádu φ je kanonická, pokud

- φ má formu $(\forall u)[\bar{K}_1 \vee \ldots \vee \bar{K}_m]$, kde $K_1, \ldots, K_m$ jsou klausule (*konstituční klausule φ*), a

- konstanty (respektive proměnné) formule φ, je původní segment v lexikografickém pořadí konstant (resp. proměnných).

Důkaz rozhodnutelnosti

Důkaz. Nechť φ_0 je Shelahova sentence. Bez ztráty obecnosti φ_0 obsahuje všeobecný kvantifikátor, takže se prefix φ skládá ze dvou existenčních kvantifikátorů separovaných kvantifikátorem všeobecným. Odstraňte první dávku a nahraďte odpovídající proměnné konstantami v části sentence, která je bez kvantifikátorů. Nechť φ je výslednou sentencí. Očividně je φ splnitelná tehdy a právě tehdy, když je splnitelná φ_0.

Ve zbytku důkazu provádím několik transformací na φ, než dostaneme kanonickou sentenci. V každém případě je výstup ekvivalentní vstupu a vstup i výstup budou označeny φ. Přemýšlejte o φ jako o aktuální formuli.

Transformace 0: *Začátek*. Transformujte tu část QF(φ) z φ, která je bez kvantifikátoru, na ekvivalentní formuli bez kvantifikátoru, která je postavena na literálech metodami konjunkce a disjunkce. Tyto literály se budou nazývat konstitučními literály φ. Pro každý literál α nechť platí, že Hloubka(α) je sumou hloubek konstitučních termů α.

Transformace 1: *Redukce hloubky termů*. Nechť *I* je kolekcí nepřípustných konstitučních literálů z φ a zároveň $d = \Sigma_{\alpha \in I}$ Hloubka(α). Pokud $d > 0$, zvolte podterm Par(t) hloubky 1 z termu v *I* a nahraďte QF(φ) za

$(\exists v)[v = \text{Par}(t) \wedge \varphi']$,

kde *v* je nová existenční proměnná a φ′ je výsledek náhrady Par(*t*) za proměnnou *v* v QF(φ). Opakujte tuto proceduru, než $d = 0$.

Transformace 2: Eliminace nepřípustných konstitučních literálů. Redukujte QF(*φ*) na disjunktivní normální formu. Nechť *I* je potom kolekcí nepřípustných konstitučních literálů *φ*. Je velmi snadné zpozorovat, že každé $\alpha \in I$, je rovností. Pokud $I \neq \emptyset$, zvolte literál $t = t'$ v *I*. Bez ztráty obecnosti platí, že *t* předchází v lexikografickém pořadí *t*′. Pro každý term disjunkce z QF(φ), který má zvolený literál, jako komponentu konjunkce, proveďte následující: vymažte zvolenou komponentu konjunkce a nahraďte *t*′ za *t,* ve zbývajících termech konjunkce. Opakujte tuto proceduru, až bude platit, že $I = \emptyset$.

Transformace 3: Závěr: užijte ekvivalencí

$(\exists v)(\alpha \vee \beta) \equiv (\exists v)\alpha \vee (\exists v)\beta$ a $(\exists v)(\gamma) \equiv \gamma$,

kde γ neobsahuje *v* k tomu, abyste transformovali φ do formy kanonické sentence.

Příklady

Následují příklady, kdy zadaná formule nesplňuje podmínky Shelahovy třídy. Důkazovým postupem tak nerozhodneme danou formuli.

Protipříklad:

$\forall x[\neg(P(x) \supset \exists z(\neg\forall y[Q(x, y) \supset P(f(v))])) \vee \exists y(Q(x, y) \supset P(x))]$ – Výchozí formule

U toho příkladu je patrné, že nesplňuje podmínky Shelohovi třídy. Můžeme si ukázat důkaz této formule.

Skolemizace
$\forall x[\neg(P(x) \supset \exists z(\neg\forall y[Q(x, y) \supset P(f(v))])) \vee \exists y(Q(x, y) \supset P(x))] \Leftrightarrow$ (*negace formule*)

$\neg\{\forall x[\neg(P(x) \supset \exists z(\neg\forall y[Q(x, y) \supset P(f(v))])) \vee \exists y(Q(x, y) \supset P(x))]\} \Rightarrow$ (*eliminace nadbytečných a zavedení nových kvantifikátoru*)

$\neg\{\exists v\forall x[\neg(P(x) \supset (\neg\forall y[Q(x, y) \supset P(f(v))])) \vee \exists y(Q(x, y) \supset P(x))]\} \Leftrightarrow$ (*přejmenování prom.*)

$\neg\{\exists v\forall x[\neg(P(x) \supset (\neg\forall y[Q(x, y) \supset P(f(v))])) \vee \exists y_1(Q(x, y_1) \supset P(x))]\} \Leftrightarrow$ (*eliminace implikace*)

$\neg\{\exists v\forall x[\neg(\neg P(x) \vee (\neg\forall y[\neg Q(x, y) \vee P(f(v))])) \vee \exists y_1(\neg Q(x, y_1) \vee P(x))]\} \Leftrightarrow$ (*přesun $\neg$ dovnitř*)

$\neg\{\exists v\forall x[(P(x) \wedge (\forall y[\neg Q(x, y) \vee P(f(v))])) \vee \exists y_1(\neg Q(x, y_1) \vee P(x))]\} \Leftrightarrow$ (*přesun $\neg$ dovnitř*)

$\exists v\forall x[(\neg P(x) \vee (\exists y[Q(x, y) \wedge \neg P(f(v))])) \wedge \forall y_1(Q(x, y_1) \wedge \neg P(x))]\} \Rightarrow$ (*eliminace $\exists$*)

$\forall x[(\neg P(x) \vee ([Q(x, g(x)) \wedge \neg P(f(a))])) \wedge \forall y_1(Q(x, y_1) \wedge \neg P(x))] \Leftrightarrow$ (*přesun kvant. doleva*)

$\forall x\forall y_1[(\neg P(x) \vee (Q(x, g(x)) \wedge \neg P(f(a)))) \wedge Q(x, y_1) \wedge \neg P(x)] \Leftrightarrow$ (*distributivní zákony*)

$\forall x\forall y_1[(\neg P(x) \vee Q(x, g(x)) \wedge (\neg P(x) \vee \neg P(f(a)))) \wedge Q(x, y_1) \wedge \neg P(x)]$

Rezoluce

1. $\neg P(x) \vee Q(x, g(x))$
2. $\neg P(x) \vee \neg P(f(a))$
3. $Q(x, y_1)$
4. $\neg P(x)$

Tyto resolventy nelze nijak unifikovat, tudíž jsme nedošli ke sporu a původní formule není tautologie.

Protipříklad 2:

$\exists x\exists y[P(x,y) \wedge \forall r\ \neg Q(x,r)] \vee \forall s\forall t\exists z[\neg P(s,t) \vee Q(t,z) \vee [Q(s,z) \wedge P(t,z)]]$ – Výchozí formule

Převedeme všechny kvantifikátory na levou stranu (začátek formule) a tím získáme prenexní tvar této formule.

$\exists x\exists y\forall r\forall s\forall t\exists z\ ([P(x,y) \wedge \neg Q(x,r)] \vee [\neg P(s,t) \vee Q(t,z) \vee [Q(s,z) \wedge P(t,z)]])$ – prenexní tvar

Jak je vidět tato formule rozhodně nesplňuje podmínky Shelahovy třídy – neobsahuje požadovaný prefix a navíc neobsahuje symbol rovnosti. Provedeme tedy negaci původní formule a vyzkoušíme si její důkaz.

Skolemizace

$\exists x\exists y[P(x,y) \wedge \forall r\ \neg Q(x,r)] \vee \forall s\forall t\exists z\ [\neg P(s,t) \vee Q(t,z) \vee [Q(s,z) \wedge P(t,z)]] \Leftrightarrow$ (*negace formule*)

$\forall x\forall y[\neg P(x,y) \vee \exists r\ Q(x,r)] \wedge \exists s\exists t\forall z[P(s,t) \wedge \neg Q(t,z) \wedge [\neg Q(s,z) \vee \neg P(t,z)]] \Rightarrow$ (*eliminace $\exists$*)

$\forall x \forall y[\neg P(x,y) \vee Q(x,f(y))] \wedge \forall z[P(a,b) \wedge \neg Q(b,z) \wedge [\neg Q(a,z) \vee \neg P(b,z)]] \Leftrightarrow$ (*přesun kvantifikátorů doleva*)

$\forall x \forall y \forall z[(\neg P(x,y) \vee Q(x,f(y))) \wedge P(a,b) \wedge \neg Q(b,z) \wedge (\neg Q(a,z) \vee \neg P(b,z))]$

Rezoluce

1. $\neg P(x,y) \vee Q(x,f(y))$
2. $P(a,b)$
3. $\neg Q(b,z)$
4. $\neg Q(a,z) \vee \neg P(b,z))$
5. $Q(a,f(b))$ rezoluce 1, 2 a/x b/y
6. $\neg P(b, f(b))$ rezoluce 4, 5 z/f(b)

Nelze dále unifikovat. Proto původní formule není tautologií (nedošli jsme ke sporu).

5 Závěr

Hlavním cílem mé diplomové práce bylo zmapování problematiky týkající se logické pravdivosti formulí v predikátové logice prvního řádu a zároveň zpracování přehledné studie o této problematice. V českém jazyce bychom těžko hledali studii, která by se zabývala právě rozhodnutelnými podtřídami formulí PL1. Z dostupných materiálů – především v angličtině - se mi podařilo zjistit, že existuje 7 maximálních tříd, ve kterých je logická pravdivost formulí predikátové logiky prvního řádu rozhodnutelná. Tyto třídy (fragmenty) se vztahují jak na predikátovou logiku bez rovnosti, tak i na predikátovou logiku s rovností.

V krátkosti se pokusím shrnout obsah celé diplomové práce.

V první části diplomové práce jsem definoval důležité pojmy, které souvisí s predikátovou logikou prvního řádu. Zabýval jsem se tak obecným výkladem jazyka PL1, monadickou predikátovou logikou či predikátovou logikou s rovností. Nastínil jsem také rezoluční metodu, jako důkazový postup, který využívám v příkladech.

Další část této práce byla věnována obecnému problému nerozhodnutelnosti predikátové logiky prvního řádu. V této kapitole jsem – mimo jiné – představil 16 standardních tříd, ve kterých je problém logické pravdivosti nerozhodnutelný a popsal jsem i další nerozhodnutelné aritmetiky. Ukázali jsme si, že predikátová logika je vlastně částečně (parciálně) rozhodnutelná.

Poslední kapitola ukázala rozhodnutelné třídy (fragmenty) formulí PL1. V prvé řadě se jedná o Löb-Gurevichovu třídu, která obsahuje pouze monadické predikáty, tudíž se vlastně jedná o monadickou predikátovou logiku. Další z těchto tříd je Gödel-Kalmár-Schütteova třída, která má v prenexním tvaru prefix $\exists^*\forall^2\exists^*$ a neobsahuje žádné funkční symboly. Velmi podobná je pak Bernays-Schönfinkelova třída, u níž je prefix v prenexní normální formě ve tvaru $\exists^*\forall^*$. Taktéž jako Gödel-Kalmár-Schütteova třída nesmí formule obsahovat funkční symboly či další kvantifikátory. Tyto dvě třídy jsou maximální rozhodnutelné prefixové třídy v čisté predikátové logice (predikátový kalkul bez rovnosti a funkčních symbolů). Pomyslnou čtveřici rozhodnutelných tříd bez rovnosti, pak uzavírá Gurevich-Maslov-Orevkovova třída – její prefix je ve tvaru $\exists^*\forall\exists^*$ a na rozdíl od předešlých tříd není nijak omezená do počtu funkčních nebo relačních symbolů.

Dále se v práci zabývám rozhodnutelnými třídami pro predikátovou logiku s rovností. První z nich je Gurevichova třída. Omezení této třídy spočívá v prefixu, který musí být ve tvaru $\exists^*$. Formule – splňující omezení Gurevichovy třídy - musí dále obsahovat buďto dva funkční symboly nebo funkční a relační symbol či funkci s aritou, která je větší než jedna. Následuje Rabinova třída, která nemá omezení ve formě prefixu, ale daná formule musí obsahovat jednu unární funkci a pouze monadické predikáty. Poslední sedmou třídou je pak Shelahova třída. Formule, která by měla splňovat omezení této třídy, musí mít prefix v prenexní normální formě ve tvaru $\exists^*\forall\exists^*$. Formule – splňující dané omezení - dále neobsahuje žádné funkční symboly s aritou vetší nebo rovno 2 a obsahuje nejvýše jeden unární funkční symbol. U Shelahovi třídy neplatí žádné omezení na počet predikátů či jejich arit.

Celá diplomová práce je ve stručnější a přehlednější podobě zpracována i ve formě webové stránky na adrese www.rozhodnutelne-tridy.cz. Tyto stránky by měly soužit především jako učební pomůcka pro studenty předmětu *vybrané partie z matematické logiky*. Věřím však, že pomohou i dalším lidem, které problematika rozhodnutelnosti formulí v predikátové logice prvního řádu zajímá.

Literatura

1. *Decidability (logic) – Wikipedia, the free encyclopedia.* [Online] 17. září 2011. <http://en.wikipedia.org/wiki/Decidability_(logic)>.

2. Egon Börger, Erich Grädel, Yuri Gurevich - The Classical Decision Problem. Springer, 2001.

3. Vítězslav Švejdar – LOGIKA neúplnost, složitost a nutnost. ISBN 80-7042-856-2.

4. *Bernays–Schönfinkel class – Wikipedia, the free encyclopedia.* [Online] 22. duben 2011. <http://en.wikipedia.org/wiki/Bernays–Schönfinkel_class>.

5. František Včelař, Jaroslav Frýdek, Ivan Zelinka – Gödel 1931. ISBN 978-80-7300-247-3.

6. Erich Grädel - Decidable Fragments of First-Order and Fixed-Point Logic (From prefix-vocabulary classes to guarded logics). [Online]. <http://www-mgi.informatik.rwth-aachen.de/~graedel/kalmar.pdf>.

7. Viorica Sofronie-Stokkermans - Undecidability and Decidability Result [Online]. <http://www.mpi-inf.mpg.de/~sofronie/lecture-ar-09/slides/lecture-17-june.pdf>.

8. *Entscheidungsproblem – Wikipedia, the free encyclopedia.* [Online] 21. březen 2012. <http://en.wikipedia.org/wiki/Entscheidungsproblem>.

9. R. Ramanujam - Decidable fragments of first order logic [Online]. < http://fmindia.cmi.ac.in/update2008/slides/R._Ramanujam_jam.pdf>.

10. Aleksandr Aleksandrovich Markov - Matematická logika a numerická analysa. Pokroky matematiky, fyziky a astronomie, Vol. 3 (1958), No. 5, 516—519 [Online]. <http://dml.cz/dmlcz/139961>.

11. Jiří Hořejš; Alois Glanc - O vztahu formy a obsahu v matematice a logice. II. Pokroky matematiky, fyziky a astronomie, Vol. 12 (1967), No. 2, 67--84 [Online]. <http://dml.cz/dmlcz/137063>.

12. Marie Duží - Logika pro informatiky (a příbuzné obory), skripta.

13. Presburger Arithmetic - Wolfram MathWorld. [Online]. <http://mathworld.wolfram.com/PresburgerArithmetic.html>.

14. *Presburgerova aritmetika – Wikipedia, the free encyclopedia.* [Online] 26. únor 2012. <http://cs.wikipedia.org/wiki/Presburgerova_aritmetika>.

15. Jirí Velebil - Velmi jemný úvod do matematické logiky (Doplňkový text k přednáškám Y01MLO a X01DML). České Vysoké Učení Technické v Praze, Fakulta elektrotechnická, 2007. [Online]. <ftp://math.feld.cvut.cz/pub/velebil/y01mlo/logika.pdf>.

16. Petr Hájek a Vítězslav Švejdar - MATEMATICKÁ LOGIKA (Předběžný studijní text), 1994. [Online]. <http://www1.cuni.cz/~svejdar/papers/mate94.pdf>

17. W. Ackermann – solvable cases of the decision problem (North-Holland Publishing Company, 1954).

18. *Monadic predicate calculus – Wikipedia, the free encyclopedia.* [Online] 11. prosinec 2011. <http://en.wikipedia.org/wiki/Monadic_logic>.

19. *Gödelovy věty o neúplnosti – Wikipedia, the free encyclopedia.* [Online] 25. ledna 2012. <http://cs.wikipedia.org/wiki/G%C3%B6delovy_v%C4%9Bty_o_ne%C3%BAplnosti>.

20. Salvatore Ruggieri - (Un)decidability problems in first order logic. [Online]. <http://personnel.univ-reunion.fr/fred/Enseignement/CalculComplex/SRslides.pdf>

21. Yuri Gurevich - On the Classical Decision Problem. MI 48109-2122. [Online]. <http://research.microsoft.com/en-us/um/people/gurevich/Opera/91.pdf>.

22. D. Hilbert and P. Bernays. Grundlagen der Mathematik. Springer-Verlag, Berlin, Band I (1934, 1968), Band II (1939, 1970).

23. M. Davis, Y. Matijasevich, and J. Robinson. Hilbert's tenth problem. Diophantine equations: Positive aspects of negative solutions. In AMSProceedings of Symposia in Pure Mathematics, pages 323–378, 1976.

24. E. Börger. Computability, Complexity, Logic. Studies in Logic and the Foundations of Math., 128, 1989. North-Holland.

25. H.-D. Ebbinghaus, J. Flum, and W. Thomas. Mathematical Logic. Springer, 1984.

26. H. Enderton. A Mathematical Introduction to Logic. Academic Press, 1972.

27. S. Kleene. Introduction to Metamathematics. Elsevier, North-Holland, 1952.

28. J. Shoenfield. Mathematical Logic. Addison-Wesley, 1967.

29. P. Bernays and M. Schönfinkel. Zum Entscheidungsproblem der mathematischen Logik. Math. Annalen, 99:342–372, 1928.

30. F. Ramsey. On a problem of formal logic. Proc. of the London Math. Soc.2nd series, 30:264–286, 1930.

31. G. Frege. Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens. 1879.

32. Marie Duží - Kurt Gödel. Metamathematical results on formally undecidable propositions: Completeness vs. Incompleteness. [Online]. <http://www.cs.vsb.cz/duzi/goedel.pdf>

33. Antonín Sochor - Logika pro studenty středních škol. [Online]. <http://www.cs.vsb.cz/duzi/Logika.pdf>

34. Klaus Ambos-Spies - Decidable fragments of first-order logic. [Online]. <http://www.math.uni-heidelberg.de/logic/md/lehre/ra41-forallexists-41.pdf>

35. Filip Tvrdý - Turingův test, Filosofické aspekty umělé inteligence (Disertační práce). [Online]. <http://www.kfil.upol.cz/doc/pgs/tvrdy/Disertacni_prace.pdf>

36. Antonín Sochor - VĚTY O NEÚPLNOSTI. [Online]. <http://www.math.cas.cz/~sochor/kniha.free/gl-228-262.pdf>

37. *Rozhodnutelnost - Wikipedia, the free encyclopedia.* [Online] 7. července 2011. <http://cs.wikipedia.org/wiki/Rozhodnutelnost>

38. Nerozhodnutelnost, neúplnost (Meze formální metody). [Online]. <http://kti.ms.mff.cuni.cz/teaching/files/materials/PL5_1.pdf >

39. Y. Gurevich. On the classical decision problem. In G. Rozenberg and A. Salomaa, editors, Current Trends in Theoretical Computer Science, stránky 254 – 265. World Scientific, 1993.

40. Petr Štěpánek - Výroková a predikátová logika podrobně (záznam z přednášek převyprávěl Jan Pelc), 2008. [Online]. <http://www.ms.mff.cuni.cz/~pelcj6am/vpl_text.pdf>

41. B. Dreben and W. Goldfarb. The decision problem: solvable cases of quantificational formulas. Addison-Wesley, 1979.

42. H. Lewis. Unsolvable Classes of Quantificational Formulas. Addison-Wesley, 1979.

43. *Robinsonova aritmetika – Wikipedia, the free encyclopedia.* [Online] 18. ledna 2011. <http://cs.wikipedia.org/wiki/Robinsonova_aritmetika>.

44. Aaron R. Bradley - First-Order Theories. [Online]. <http://theory.stanford.edu/~arbrad/slides/cs156-old/lec3-4.pdf>

45. Monadic logic - Signature only monadic (unary) redicates. [Online]. <http://www.cs.tau.ac.il/~rabinoa/logic6-1-04.pdf>

46. J. Herbrand. Sur le probleme fondamental de la logique mathématique, volume 24, pages 12–56.

47. Petr Štěpánek - Predikátová logika (prezentace k přednášce Výroková a predikátová logika). [Online]. <http://kti.mff.cuni.cz/teaching/files/materials/StepanekPetr_PredikatovaLogika_2x2.pdf>

48. K. Gödel. Zum Entscheidungsproblem des logischen Funktionenkalkuls. Monatshefte f. Mathematik u. Physik, 40:433–443, 1933. Reprinted in [188, pp. 306–326]

49. William H. Joyner JR. - Resolution Strategies as Decision Procedures. [Online]. <http://www.cs.famaf.unc.edu.ar/~careces/cordoba08/Bib/joyner.pdf>

50. Marie Demlová - Příklady k předmětu Matememattická logika. [Online]. <http://math.feld.cvut.cz/scholtzova/mlo/06-prikl-prezol.pdf>

51. J. Mlček – Výroková a predikátová logika. [Online]. <http://kti.mff.cuni.cz/~mlcek/PART_11.pdf>

52. Farn Wang (Dept. of Electrical Engineering National Taiwan University) - Predicate Calculus Formal Methods. [Online]. <http://cc.ee.ntu.edu.tw/~farn/courses/FMV/formal.methods.05.predicate.logics.pdf>

53. James Hein (Portland State University) - Lecture Notes. [Online] <http://web.cecs.pdx.edu/~jhein/lectures/ >

54. Charles Jordana, Thomas Zeugmanna - Testable and Untestable Classes of First-Order Formulae. [Online]. <http://www-alg.ist.hokudai.ac.jp/~skip/pub/jcss12.pdf >

55. Alena Lukasová - LOGIKA PRO UČITELE I, 2003. [Online]. ISBN 80-7042-856-2. <http://informatikaou.wz.cz/1-logika_pro_ucitele-lukasova-skripta.pdf>

56. Petr Štěpánek - Predikátová logika (Skripta pro přednášku Výroková a predikátová logika), 2000. [Online]. <http://kti.ms.mff.cuni.cz/teaching/files/materials/StepanekPetr_PredikatovaLogika.pdf>

Adresářová struktura přiloženého DVD

/texty – složka obsahující soubory s textem práce, zadáním, klíčovými slovy a abstraktem.

/texty/rozhodnutelne-podtridy-formuli-pl1-vas267.pdf - kompletní diplomová práce ve formátu PDF/A.

/texty/rozhodnutelne-podtridy-formuli-pl1-vas267.docx - kompletní diplomová práce ve formátu docx.